Kelvin Open Science Publishers
Connect with Research Community

Commentary *Volume 2 | Issue 1*

KOS Journal of AIML, Data Science, and Robotics
https://kelvinpublishers.com/journals/aiml-data-science-robotics.php

Hybrid Cloud, Cybersecurity, and Artificial Intelligence in Healthcare: A Strategic Convergence for U.S. Critical Infrastructure and National Competitiveness

Tirumala Ashish Kumar Manne*

Principal Cloud Architect, Optum, Eden Prairie, USA

***Corresponding author:** Tirumala Ashish Kumar Manne, Principal Cloud Architect, Optum, Eden Prairie, USA

Received: March 18, 2026; **Accepted:** April 01, 2026' **Published:** April 03, 2026

Citation: Tirumala AKM. (2026) Hybrid Cloud, Cybersecurity, and Artificial Intelligence in Healthcare: A Strategic Convergence for U.S. Critical Infrastructure and National Competitiveness. *KOS J AIML, Data Sci, Robot.* 2(1): 1-4.

1. Abstract

The convergence of hybrid cloud computing, cybersecurity, and artificial intelligence (AI) in healthcare constitutes a field of demonstrable U.S. national importance. Healthcare and Public Health is federally designated as one of sixteen critical infrastructure sectors, and recent large-scale cyberattacks including the 2024 Change Healthcare ransomware incident, which compromised the protected health information of approximately 190 million individuals have exposed systemic vulnerabilities in the digital infrastructure upon which care delivery, payment processing, and population-level health operations depend. This commentary argues that secure hybrid-cloud architecture, zero-trust cybersecurity, and responsibly governed AI should be understood not as routine enterprise technology concerns but as strategic national capabilities. The argument draws on Executive Order 14028 on cybersecurity, Executive Order 14179 on AI leadership, HHS sector designations, OMB modernization memoranda, and empirical breach data to demonstrate that resilient digital health infrastructure directly serves U.S. public safety, economic competitiveness, and population health.

2. Keywords: Hybrid Cloud, Cybersecurity, Artificial Intelligence, Healthcare, Critical Infrastructure, Zero Trust, Digital Resilience, Patient Safety, National Competitiveness, Secure Cloud Modernization

3. Introduction

Healthcare in the United States has become inseparable from its digital infrastructure. Electronic health records, payer-provider data exchange, claims processing platforms, telehealth services, pharmacy benefit systems, and AI-enabled clinical workflows now form the operational backbone through which hundreds of millions of Americans access treatment, benefits, and continuity of care. The strategic question confronting the field is no longer whether healthcare organizations will modernize their digital foundations, but whether they can do so with the security, resilience, and governance that a critical infrastructure sector demands.

Federal policy already provides the essential framing. Executive Order 14028 acknowledges that the United States faces persistent and increasingly sophisticated cyber campaigns and calls for bold changes and significant investments to protect systems that are cloud-based, on-premises, or hybrid [1]. When applied to healthcare, this directive places secure digital modernization within a framework of national and economic security. Executive Order 14179 further declares it the policy of the United States to sustain and enhance American leadership in artificial

intelligence to promote economic competitiveness and national security [8]. Together, these instruments establish that the intersection of cybersecurity, cloud modernization, and AI is not a narrow technical specialty but a domain of national strategic importance.

This commentary argues that the combined field of hybrid cloud, cybersecurity, and AI in healthcare meets the threshold of U.S. national importance based on three interrelated premises: 1) healthcare is federally recognized critical infrastructure whose digital failures carry population-scale consequences; 2) recent empirical evidence demonstrates that those consequences are not hypothetical; and 3) federal policy explicitly ties cybersecurity resilience, secure cloud adoption, and AI leadership to national competitiveness and public safety.

4. Healthcare as Population-Scale Critical Infrastructure

The U.S. Department of Health and Human Services (HHS) designates the Healthcare and Public Health (HPH) sector as one of the nation's sixteen critical infrastructure sectors [2]. This designation carries significant implications: scheduling systems, claims platforms, prior authorization workflows, eligibility verification, care management tools, pharmacy interfaces, and clinical record systems are not isolated local conveniences but components of the digital machinery through which millions of people access care, benefits, and reimbursement.

HHS has stated that its cybersecurity performance goals are designed to help the HPH sector prepare for and respond to cyber threats, build resilience, and protect patient health information and safety [3]. HHS preparedness guidance further describes operational scenarios in which cyber disruptions lead to ambulance diversions, cancellation of elective procedures, regional outages affecting nearby facilities, and disruptions to patient portals and medical-record access [4]. These are not merely technical failures; they are service-delivery failures that affect care access, patient throughput, and public health response at population scale.

Congressional testimony from HHS officials has reinforced this framing, characterizing healthcare cybersecurity as a matter requiring dedicated capability, resources, and sector-wide coordination [5]. When the sector is understood through this lens, resilient digital architecture becomes a matter of national consequence rather than institutional preference.

5. Empirical Evidence: The Scale of Digital Vulnerability

The national significance of this field is not merely a policy argument; it is empirically demonstrable. In February 2024, the ransomware group ALPHV/BlackCat attacked Change Healthcare, a subsidiary of UnitedHealth Group that processes approximately 15 billion health care transactions annually [12]. The attack encrypted and incapacitated significant portions of the company's functionality, and the compromised system lacked multi-factor authentication on a critical remote-access portal [12]. As of July 2025, HHS confirmed that approximately 192.7 million individuals were impacted, making it the largest healthcare data breach in history [13].

The operational consequences were immediate and far-reaching. A March 2024 American Hospital Association survey of nearly 1,000 hospitals found that 74% reported direct impacts on patient care, 94% reported financial impacts, one-third reported disruption to more than half their revenue, and 60% required two weeks to three months to resume normal operations [12]. An American Medical Association survey found that 80% of physician practices lost revenue from unpaid claims and 60% faced challenges verifying patient eligibility [14]. The total cost to UnitedHealth Group reached an estimated $2.457 billion through the third quarter of 2024 [15].

The Change Healthcare incident was not an isolated event. In 2024, there were 14 data breaches each involving more than one million healthcare records, and the records of approximately 277 million U.S. residents were exposed or compromised across all reported breaches [16]. Healthcare endured 444 reported cyberthreat incidents in 2024, including 238 ransomware attacks and 206 data breach events-more than any other critical infrastructure sector [17]. In 2025, at least 57 million additional individuals were affected by healthcare breaches [18]. These figures confirm that digital vulnerability in healthcare operates at a scale commensurate with national infrastructure, not individual enterprise risk.

6. Hybrid Cloud as the Foundation for Secure Modernization

Hybrid cloud is especially important in healthcare because healthcare workloads are heterogeneous. Some workloads require the elasticity and rapid service deployment of public cloud environments. Others require tighter latency control, data-locality choices, specialized integrations, or retention of private infrastructure due to operational, contractual, or regulatory considerations. The practical modernization path is therefore rarely all-cloud or all-on-premises; it is governed coexistence across multiple environments.

This architecture aligns closely with the federal modernization model. Executive Order 14028 explicitly addresses the protection of systems whether cloud-based, on-premises, or hybrid [1]. The Office of Management and Budget's FedRAMP modernization memorandum (M-24-15) explains that FedRAMP exists to safely accelerate cloud adoption while promoting consistent security assessment across the federal enterprise [6]. Although directed at federal agencies, the policy logic applies equally to healthcare: modernization should accelerate capability without relaxing security expectations.

In practical terms, hybrid cloud enables healthcare organizations to modernize incrementally rather than disruptively. It supports workload portability, disaster-recovery planning, identity federation, API-driven interoperability, and the scaling of analytics or AI workloads without forcing every core clinical system into a single environment. The Change Healthcare breach underscored precisely this point: consolidation without resilient, distributed architecture creates systemic single points of failure [12]. Secure hybrid cloud directly mitigates that risk.

7. Cybersecurity Resilience and Zero-Trust Architecture

Cybersecurity in healthcare must be understood as a resilience discipline, not merely a compliance exercise. Healthcare organizations are high-value targets because they handle sensitive personal data, support essential public

services, depend on complex third-party ecosystems, and often operate mixed environments with both modern and legacy assets. When those environments are compromised, the resulting disruption is simultaneously operational, clinical, legal, and reputational.

Executive Order 14028 states that prevention, detection, assessment, and remediation of cyber incidents are essential to national and economic security [1]. OMB Memorandum M-22-09 articulates the federal zero-trust strategy, requiring stronger cybersecurity baselines to defend against campaigns that threaten public safety, privacy, the economy, and trust [7]. Zero trust-with its emphasis on identity-centric controls, continuous verification, enterprise logging, and workload-level protection-represents a nationally important design paradigm rather than an optional best practice.

The empirical record reinforces this urgency. The Change Healthcare breach exploited a remote-access portal that lacked multi-factor authentication-a basic zero-trust control [12]. Over 80% of stolen protected health information records in recent years were taken not from hospitals directly but from third-party vendors and business associates [17]. These patterns demonstrate that cybersecurity resilience in healthcare requires architecturally embedded controls across the full ecosystem, not perimeter-based defenses around individual organizations.

8. Artificial Intelligence, Enterprise Transformation, and U.S. Competitiveness

Artificial intelligence amplifies the national significance of this field in two ways. First, AI can materially improve healthcare operations-identifying risk, prioritizing work, reducing administrative friction, detecting anomalies, and enabling more responsive decision support. The global AI in healthcare market, estimated at approximately $37 billion in 2025, is projected to exceed $500 billion by 2033, with North America accounting for over 54% of revenue [19]. Second, AI introduces new governance, trust, and security demands. Models require high-quality data, secure development pipelines, auditable deployment patterns, and robust controls around access, integrity, and monitoring. In healthcare, AI without secure infrastructure is not scalable innovation; it is unmanaged exposure.

Current U.S. policy explicitly frames AI as a competitiveness issue. Executive Order 14179 declares it the policy of the United States to sustain and enhance American global AI dominance in order to promote human flourishing, economic competitiveness, and national security [8]. The White House's AI Action Plan adds that the United States must innovate rapidly in AI, establish American AI as a gold standard, and capture AI-enabled gains including breakthroughs in medicine [9]. These documents establish that secure AI deployment in healthcare is part of a nationally important domain tied to economic competitiveness and strategic technological leadership.

This is also where enterprise digital transformation becomes inseparable from cyber and cloud architecture. AI value in healthcare does not emerge from the model alone. It depends on governed data movement, interoperable platforms, secure cloud resources, robust identity controls, and operational trust. The field is nationally important precisely because it connects high-value AI adoption with the resilient digital foundations required to use it responsibly.

9. Protection of Healthcare and Financial Data

Healthcare is increasingly interconnected with financial and administrative ecosystems, including billing, claims, fraud detection, payment operations, benefits administration, and vendor networks. This interconnection means the field also touches the protection of healthcare and financial data together. The Change Healthcare breach, for example, compromised not only medical records but also billing records, payment card information, and financial and banking records [15].

Treasury's Office of Cybersecurity and Critical Infrastructure Protection works to enhance the security and resilience of financial services sector infrastructure and reduce operational risk [10]. Treasury's Cloud Executive Steering Group highlights frameworks for secure cloud implementation and baseline security outcomes for critical infrastructure entities [11]. Although the financial sector is distinct from healthcare, these sources reinforce a larger point: secure cloud modernization and cyber resilience are core concerns wherever essential services depend on sensitive data and interconnected digital infrastructure.

10. Conclusion

The convergence of hybrid cloud, cybersecurity, and artificial intelligence in healthcare should be understood as an integrated field of U.S. national importance. Federal policy provides the essential rationale: The nation must protect critical digital infrastructure, modernize securely across cloud and hybrid environments, build cyber resilience, protect sensitive data, and preserve leadership in AI [1,6-9]. Healthcare sits directly inside that agenda because it is critical infrastructure and because digital failures in healthcare-as the Change Healthcare breach and the broader empirical record demonstrate-disrupt safety, access, continuity, and trust at population scale [2-5,12-18].

Work at this intersection should be viewed not as routine information technology activity, but as strategically important work that advances U.S. public safety, enterprise transformation, and national competitiveness. As AI adoption accelerates, as cloud environments grow more complex, and as cyber threats become more sophisticated, the professionals and institutions that build resilient digital health infrastructure are contributing directly to the nation's capacity to deliver safe, effective, and trustworthy healthcare at scale.

11. Conflict of Interest Statement

The author declares no conflicts of interest relevant to this commentary.

12. Funding

This work received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

13. References

1. Executive Order 14028-Improving the Nation's Cybersecurity. Administration of Joseph R. Biden, Jr., May 12, 2021. Available from: https://www.govinfo.gov/link/cpd/executiveorder/14028
2. Executive Order 14179-Removing Barriers to American Leadership in Artificial Intelligence. The White House, January 23, 2025. Available from:

https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/
3. About the HPH Sector. U.S. Department of Health and Human Services, ASPR. Available from: https://aspr.hhs.gov/HPH-Sector/Pages/About.aspx
4. HHS Cybersecurity Performance Goals. U.S. Department of Health and Human Services. Available from: https://hhscyber.hhs.gov/performance-goals.html
5. Healthcare System Cybersecurity Readiness and Response Considerations. ASPR TRACIE, U.S. Department of Health and Human Services. Available from: https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf
6. HHS Testimony on Cybersecurity in Healthcare Infrastructure. U.S. Department of Health and Human Services, May 16, 2023. Available from: https://www.hhs.gov/about/agencies/asl/testimony/2023/05/2023/protecting-critical-infrastructure-from-cyberattacks.html
7. Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness. American Hospital Association, 2024. Available from: https://www.aha.org/change-healthcare-cyberattack
8. Change Healthcare Cybersecurity Incident Frequently Asked Questions. U.S. Department of Health and Human Services. Available from: https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html
9. Change Healthcare Ransomware Attack Impact. BlackFog. Available from: https://www.blackfog.com/change-healthcare-landmark-cybersecurity-breach/
10. Change Healthcare Data Breach. Krebs on Security, October 2024. Available from: https://krebsonsecurity.com/2024/10/change-healthcare-breach-hits-100m-americans/
11. The Biggest Healthcare Data Breaches of 2024. HIPAA Journal. Available from: https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024/
12. Health Care Had Most Reported Cyberthreats in 2024. American Hospital Association, May 2025. Available from: https://www.aha.org/news/headline/2025-05-12-report-health-care-had-most-reported-cyberthreats-2024
13. Largest Healthcare Data Breaches of 2025. HIPAA Journal. Available from: https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2025/
14. M-24-15: Modernizing the Federal Risk and Authorization Management Program (FedRAMP). Office of Management and Budget, July 25, 2024. Available from: https://www.whitehouse.gov/wp-content/uploads/2024/07/M-24-15-Modernizing-the-Federal-Risk-and-Authorization-Management-Program.pdf
15. M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. Office of Management and Budget, January 26, 2022. Available from: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
16. Artificial Intelligence in Healthcare Market Size and Share. Grand View Research, 2025. Available from: https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-healthcare-market
17. America's AI Action Plan. The White House, July 2025. Available from: https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf
18. Financial Institutions-Cybersecurity and Critical Infrastructure Protection. U.S. Department of the Treasury. Available from: https://home.treasury.gov/about/offices/domestic-finance/financial-institutions
19. Cloud Executive Steering Group. U.S. Department of the Treasury. Available from: https://home.treasury.gov/about/offices/domestic-finance/financial-institutions/cloud-executive-steering-group

Table 1: Key National-Interest Themes at the Intersection of Hybrid Cloud, Cybersecurity, and AI in Healthcare.

Cybersecurity resilience	Protects hospital operations, clinical systems, connected devices, and continuity of care during cyber incidents	EO 14028; HHS Cybersecurity Performance Goals [1,4]
Critical digital infrastructure	HPH is a designated critical infrastructure sector; digital resilience has national consequences	HHS HPH sector designation [3]
Healthcare and financial data protection	Sensitive records, claims, payment flows, and affiliated systems require secure architectures	HHS + Treasury guidance [3,18,19]
Secure cloud modernization	Hybrid cloud supports modernization while retaining control for regulated and mission-critical workloads	EO 14028; FedRAMP modernization [1,14]
Zero-trust architecture	Identity-centric controls, continuous verification, and workload-level protection across hybrid environments	OMB M-22-09 [15]
Economic competitiveness and AI leadership	AI-enabled health operations and secure deployment align with U.S. policy on AI leadership	EO 14179; AI Action Plan [2,17]