

REVIEWER'S REPORT

Manuscript No.: IJAR- 59223

Title: Cloud-Based Healthcare Information Infrastructure for Secure and Scalable Digital Health Transformation in Saudi Arabia,

Recommendation:

Accept after minor revision

Rating	Excel.	Good	Fair	Poor
Originality		✓		
Techn. Quality			✓	
Clarity			✓	
Significance	✓			

Reviewer's ID: Biquees Hamza

Detailed Reviewer's Repot

The manuscript presents a structured integrative literature review focusing on cloud-based healthcare information infrastructure as a critical foundation for Saudi Arabia's national digital health strategy under Vision 2030. Modern healthcare delivery has evolved into a data-intensive ecosystem where electronic health records, diagnostic imaging, virtual care platforms, mobile health applications, and connected Internet of Medical Things devices must interact seamlessly across diverse organizational boundaries. The author positions cloud computing not merely as an off-site hosting or storage solution, but as a composite architectural layer encompassing compute, storage, identity management, integration services, networking, data standards, security controls, and operational governance.

The core argument put forward is that scalability in digital health must be redefined. Rather than evaluating scalability strictly by server capacity, storage expansion, or processing speed, the review asserts that true infrastructure scalability is the capacity to expand digital services without causing a proportional increase in security risk, integration complexity, operational downtime, or governance fragmentation. Through an integrative synthesis of international informatics literature and Saudi-specific empirical adoption studies, the manuscript proposes a layered, standards-based architectural framework combined with a continuous governance model designed to guide secure and resilient cloud migrations across the Kingdom's health sector.

Evaluation of Scope, Methodological Rigor, and Conceptual Soundness

The scope of the manuscript is both timely and aligned with contemporary health informatics challenges in Saudi Arabia. As health delivery systems transition toward distributed models, virtual care, and

REVIEWER'S REPORT

predictive population health analytics, the traditional approach of relying on isolated, on-premises hospital data centers becomes an operational bottleneck. The review successfully bridges high-level health policy objectives with granular technical requirements, offering a clear conceptual link between national strategy and technical execution.

Methodologically, the paper employs a structured integrative review design informed by the systematic stages of problem definition, targeted multi-database retrieval, qualitative screening, quality appraisal, and thematic synthesis. The search strategy spans key databases, including PubMed, Scopus, Web of Science, ScienceDirect, IEEE Xplore, ACM Digital Library, and SpringerLink, targeting literature from the 2020–2025 window while retaining foundational pre-2020 framework studies where relevant.

The methodological approach exhibits several notable strengths:

- **Integrative Synthesis:** The review effectively integrates heterogeneous literature, blending empirical studies, systematic reviews, and technical computer-science research.
- **Contextual Weighting:** The author gives appropriate weight to empirical studies from Saudi Arabia to ensure that technical capabilities are interpreted through the lens of local organizational culture, workforce readiness, and regulatory compliance.
- **Methodological Transparency:** The decision to avoid reporting a retrospective, PRISMA-style numerical flowchart is methodologically sound. Because a prospectively registered screening log was not maintained, omitting arbitrary screening numbers prevents false precision while preserving transparent quality appraisal parameters.

Conceptually, treating cloud infrastructure as an interconnected ecosystem rather than isolated software applications is a major strength. The paper correctly highlights that deploying sophisticated cloud analytics or electronic health records yields limited value if underlying network latency is unmanaged, APIs lack semantic standardization, or access controls fail to follow zero-trust principles.

In-Depth Analysis of Critical Themes

Cloud Elasticity and Service Scalability

The manuscript establishes that cloud computing provides essential elasticity, allowing healthcare provider networks to provision storage and processing power dynamically. This capability is crucial for managing variable clinical workloads, such as surges in virtual consultations, continuous expansion of digital imaging archives, and periodic population-level analytical tasks. The rapid expansion of national telehealth platforms in Saudi Arabia demonstrates that digital health channels have shifted from auxiliary tools to primary care delivery infrastructure. However, the analysis rightly warns that elasticity alone does not guarantee system-level scalability. If individual hospitals migrate applications to cloud environments independently without unified standards, the result is distributed fragmentation rather than

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

enterprise integration. True scalability requires centralized identity services, shared terminology, continuous monitoring, and common security policies.

Interoperability and the Cloud Data Plane

Interoperability is identified as a strategic infrastructure requirement rather than a secondary technical integration task. The review details how modern web-based standards, specifically Fast Healthcare Interoperability Resources (FHIR) exposed through application programming interfaces (APIs), enable fluid data exchange across electronic health records, research platforms, and external services. Cloud environments are well-suited to host central API gateways, master patient indexes, terminology servers, and longitudinal data repositories. Nevertheless, the manuscript emphasizes that cloud technology cannot automatically resolve semantic inconsistencies. Without unified terminologies, standardized identifiers, and cross-organizational data governance, cross-provider information sharing remains constrained.

Cybersecurity, Zero-Trust Architecture, and Privacy

A core contribution of the manuscript is its balanced evaluation of cloud security. While centralized cloud environments offer professionalized security tooling, continuous patching, automated logging, and robust backup capabilities, centralization also expands the attack surface. Misconfigurations, credential theft, supply-chain vulnerabilities, and API compromise can impact large numbers of connected systems. To mitigate these risks, the paper advocates for a zero-trust architecture. Under zero-trust principles, every access request is continuously authenticated and authorized based on identity, device posture, and contextual role under strict least-privilege principles. Sensitive data must be classified, encrypted both in transit and at rest, and subjected to audit logging. Furthermore, privacy controls must enforce strict purpose-based data access rather than relying solely on perimeter defenses.

Internet of Medical Things (IoMT) and Edge Computing

The expansion of IoMT devices—such as remote patient monitors, wearables, bedside clinical sensors, and connected imaging tools—presents unique infrastructure challenges. Routing vast streams of continuous device telemetry directly to distant public cloud centers introduces network latency, bandwidth congestion, and service disruption risks if wide-area connectivity fails. The manuscript proposes a hybrid edge-cloud architecture as a solution. In this model, edge computing nodes stationed near clinical sites process time-critical data locally to support real-time decision-making. Selected, aggregated datasets are then synchronized with central cloud platforms for longitudinal storage, complex analytics, and model training. This distributed design ensures operational continuity even during regional network outages.

Organizational Adoption and Human Factors

REVIEWER'S REPORT

A recurring theme in the Saudi-specific evidence is that technology implementation succeeds or fails based on human and organizational factors. Digital health maturity across Saudi hospitals is deeply mediated by staff capability, organizational culture, clinical trust, and perceived usability. Cumbersome authentication procedures, slow application performance, or poorly designed administrative workflows lead clinicians to create unsafe workarounds, such as credential sharing or off-system data exports. Consequently, workforce training, role-based access design, and clinical workflow alignment must be treated as essential technical controls rather than secondary change-management activities.

Operational Resilience, Vendor Governance, and Sovereignty

The review correctly identifies availability and disaster recovery as non-negotiable requirements for healthcare systems, where service outages directly threaten patient safety. Cloud architectures must incorporate redundant availability zones, immutable backups, offline clinical procedures, and routinely tested recovery plans. Additionally, the manuscript addresses vendor lock-in, noting that over-reliance on proprietary cloud services can restrict long-term institutional flexibility and inflate migration costs. The author recommends containerized workloads, standards-based interfaces, open data formats, and multi-layer exit strategies to retain portability. On data sovereignty, the paper redefines effective control: rather than requiring physical server ownership, meaningful sovereignty is demonstrated through transparent key management, auditable access logs, defined subcontractor boundaries, and enforceable contractual obligations.

Appraisal of Proposed Frameworks and Visual Assets

The manuscript introduces two conceptual frameworks that effectively synthesize its findings:

- 1. The Proposed Layered Architecture:** This model visualizes cloud infrastructure across four functional layers. Clinical data sources (such as electronic health records, imaging systems, telehealth portals, and IoMT devices) feed into a central Interoperability Layer built on FHIR APIs, terminology services, and identity resolution engines. This layer feeds a Hybrid Cloud Platform supplying compute, storage, analytical engines, and backup systems. These components deliver end-user Digital Services for care delivery, clinical research, and administrative operations. Crucially, Cross-Cutting Governance and Security (encompassing data classification, identity management, encryption, audit logging, resilience testing, and vendor management) intersects all four layers simultaneously, reinforcing that security is a system-wide requirement rather than a perimeter boundary.
- 2. The Continuous Governance Cycle:** This framework provides an operational roadmap for managing healthcare cloud workloads through six cyclical stages:
 - Stage 1: Classify workload and data sensitivity.

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

- Stage 2: Architect infrastructure placement and standardized interfaces.
- Stage 3: Secure identity, access controls, and data encryption.
- Stage 4: Operate, continuously monitor, and execute incident response.
- Stage 5: Test disaster recovery, failover systems, and data portability.
- Stage 6: Reassess security risk, system performance, and clinical usability prior to repeating the cycle.

Together, these frameworks translate theoretical concepts into actionable guidance for health system executives, solution architects, and security officers.

Practical, Policy, and Future Research Implications

The practical and policy implications presented in the paper are concrete and actionable:

- **Risk-Based Workload Migration:** Healthcare organizations should categorize workloads by clinical criticality, latency tolerance, and data sensitivity before selecting deployment models (public, private, hybrid, or edge).
- **Shared Infrastructure Funding:** National policy should fund master patient indexes, terminology servers, and standardized FHIR API profiles as shared public utility infrastructure.
- **Controlled Implementation Gates:** Health enterprise managers should institute clear gate reviews—spanning inventory discovery, architectural validation, zero-trust security verification, operational support readiness, and clinical usability acceptance—before promoting cloud workloads to live environments.
- **Contractual Accountability:** Procurement teams must explicitly define responsibilities for vulnerability patching, key rotation, incident forensics, and backup verification to prevent ambiguities in vendor shared-responsibility models.

The manuscript outlines several valuable avenues for future research, including the need for longitudinal studies comparing pre- and post-migration system performance in Saudi Arabia. It also calls for empirical studies evaluating hybrid versus sovereign cloud models, operational field testing of zero-trust configurations, practical assessments of privacy-preserving federated analytics, and real-world evaluations of edge-cloud IoMT latency under variable network conditions.

Structural Critique and Specific Recommendations

While the manuscript is well-written, comprehensive, and conceptually sound, a few minor improvements would strengthen the final text:

1. **Explicit Identification of National Policy Bodies:** The manuscript refers broadly to Saudi digital health regulations and Vision 2030 objectives. Explicitly referencing key regulatory bodies—such as the Saudi Health Council (SHC), the Ministry of Health (MOH), the Saudi Data and Artificial

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

Intelligence Authority (SDAIA), and the National Cybersecurity Authority (NCA)—would provide helpful context regarding compliance requirements in the Kingdom.

- Economic and Financial Considerations:** The paper briefly notes the importance of evaluating cloud cost models. Expanding the discussion to address financial challenges—such as hidden egress fees, ongoing security tooling licensing, cost management during demand spikes, and shifting from capital expenditure (CapEx) to operational expenditure (OpEx)—would add valuable depth for healthcare financial leaders.
- Quantitative Metrics Expansion:** While the author lists useful system performance indicators (such as mean time to recovery, patch latency, and API error rates), adding recommended target ranges or benchmarks derived from international informatics standards would make these metrics even more actionable for clinical engineering teams.

Final Recommendation and Conclusion

Recommendation: Accept with Minor Revisions.

This manuscript makes a valuable contribution to the health informatics literature, providing a well-structured framework for cloud-based healthcare transformation in Saudi Arabia. By linking cloud elasticity, zero-trust security, FHIR-based interoperability, edge-IoMT design, and workforce readiness into a unified governance model, the review offers an effective roadmap for health system leaders. Addressing the minor suggestions above will further enhance the paper's clarity, policy relevance, and practical impact.