INTERNATIONAL JOURNAL OF AGEING, SAFETY, HEALTHCARE & SCIENCE INNOVATION (IJASHSI)
Vol. 03, Issue 1, September 2025, pp: 167 – 176

Post-Quantum Zero-Trust Architectures for Healthcare Data Sharing: A Roadmap for National Health Systems

Dr Samuel Owusu Nyang
University of Ghana, Accra Ghana.
Public Health in Epidemiology and Disease Control (Ph.D)
Samowusu@ug.edu.gh

ABSTRACT

The exponential digitalization of healthcare infrastructures offers remarkable potential for the collection, storage, and analysis of patient data in clinical, administrative, and research settings. This digitization, however, also exposes sensitive health information to growing cybersecurity threats. The rapid progress of quantum computing has already invalidated traditional public-key encryption schemes, while Zero-Trust Architecture (ZTA) continues to emerge as a paradigm that minimizes implicit trust and enforces strict identity management, authentication, and authorization. This article presents a strategic roadmap for the adoption of Post-Quantum Cryptography (PQC) within Zero-Trust frameworks to enable secure healthcare data sharing and analytics at the national health system level. The proposed approach integrates state-of-the-art cryptographic research, emerging secure data-sharing techniques, and innovations in population health informatics to deliver a pragmatic, evidence-based model for building resilient, scalable, and regulation-compliant infrastructures. It also provides relevant, real-world insights, use cases, and technology recommendations for national health authorities, leaders in health informatics, and security architects.

Keywords: Post-Quantum Cryptography (PQC), Zero-Trust Architecture (ZTA), Healthcare Data Security, Privacy-Preserving Computation, National Health Systems, Secure Data Sharing

INTRODUCTION

The health sector is undergoing a massive digital transformation, with burgeoning volumes of sensitive and confidential medical data being amassed, manipulated, and shared across clinical, administrative, and research environments. National health systems, from clinics and hospitals to regulatory bodies and population health platforms, are progressively digitizing operations through the deployment of electronic health records (EHRs), cloud-native digital health systems, and advanced analytics to enhance care quality, streamline resource distribution, and inform policy design. While these digital solutions offer invaluable improvements in efficiency and decision-making, they also create new vulnerabilities. Cybersecurity breaches in healthcare have grown more frequent and more severe over time, with malicious actors targeting personal health information (PHI) in bulk exfiltration campaigns for resale on black markets (Kruse et al., 2017). These breaches have significant financial and reputational implications for the affected health institutions, not to mention the long-term trust and privacy concerns for the impacted patients. In many cases, the perpetrators are opportunistic attackers seeking to exploit outdated systems and misconfigurations to maximize their gain with minimal investment (Wallace et al., 2023). In response to the increasing threats in the healthcare sector, Zero-Trust Architecture (ZTA) has begun to take root as a strategic cybersecurity architecture for many firms and national systems. ZTA is a security framework that minimizes implicit trust and automates continuous authentication and authorization (Bashar et al., 2022). It is often implemented in a microservices architecture that enforces the "least-privileged access" principle at all times. Rather than presume that internal or peripheral actors and devices in a network can be trusted implicitly, the Zero-Trust approach works on a "never trust, always verify" model. Network segmentation and micro-segmentation are employed to provide least-privileged access at the network layer, while detailed identity management, zero-trust firewalls, and real-time anomaly detection ensure strong trust management and security policy enforcement.

The Zero-Trust approach to cybersecurity, as well as the technology models in which it can be most effectively implemented, is still evolving and maturing (Fang et al., 2021). In practice, Zero-Trust is most effective at scaling trust management, monitoring human and systemic behavior, and providing consistent and reliable security policy enforcement (Jarrar, 2022). Zero-Trust approaches to cybersecurity in healthcare are best used to address known gaps, including insider threats, lateral privilege abuse, and unauthorized access to critical systems. In healthcare, this will often translate to the protection of clinical decision-support platforms, telemedicine applications, sensitive repositories such as genomic databases, and patient-facing portals.

Beyond the critical structural elements of security, Zero-Trust principles and systems must also look to cryptography to future-proof and harden their defences against future attacks. With the exponential growth of commercial and industrial quantum computing, the current ecosystem of widely used public-key cryptography, including RSA, DSA, ECC, Diffie-Hellman, and others, is at risk of retroactive decryption by adversaries with near-term or long-term quantum capabilities (Mosca, 2018). For national health systems, this risk is an existential one, as quantum adversaries could have the capacity to decrypt all sensitive patient data stored, shared, or otherwise in use over the last few decades. Ezeogu (2025a) notes that most such systems and services were built on implicit trust, and that adequately preparing for post-quantum attacks will require their early and systematic migration to post-quantum schemes such as lattice-based cryptography, multivariate quadratic equations, hash-based schemes, and others. These schemes and algorithms are already being studied, standardized, and integrated into modern products and will soon be a necessity in protecting the confidentiality of sensitive health data.

A promising research direction for building post-quantum Zero-Trust Architectures (PQ-ZTA) for national health systems is through secure computation methods that do not require actors to have trust in one another. Synthetic data generation is one of the simplest and most versatile secure computation methods. It has been shown to generate highly representative and accurate datasets for use in machine learning, research, and analytics without privacy risks of the disclosure of PHI (Ezeogu, 2025b). Synthetic data can easily be integrated into workflows across care facilities, public health agencies, and pharmaceutical and tech companies to enable safe and secure collaboration without adversaries or regulators gaining an unfair amount of trust. Similarly, secure multiparty computation (SMPC) offers strong formal privacy guarantees that multiple organizations or groups can jointly train machine learning models or perform statistical analysis without sharing raw data with one another (Ezeogu & Osigwe, 2025). Homomorphic encryption has also been proposed as a privacy-preserving technique for healthcare analytics, as it would allow encrypted data to be operated on directly, as if they were unencrypted, by third-party cloud providers and hardware accelerators (Ezeogu, 2025e).

At the highest levels, national health systems will have to grapple with architectural challenges and policy considerations when developing and maturing health ZTA. Large, decentralized, and often interoperable health systems present a challenge to blanket security policy deployment and governance, and there are costs and implications that health policy stakeholders will have to take into account. The regulatory and compliance costs of HIPAA in the United States and GDPR in the EU alone are significant and highly complex, with implied penalties and liability for affected organizations in the range of billions (Upadhya et al., 2019). While that may be the case in developed economies, it is equally, if not more, important to deploy security frameworks in low- and middle-income countries (LMICs). LMICs are heavily under-resourced and are the least capable of withstanding major security incidents, data breaches, and related healthcare downtimes. The implications of zero-trust adoption and PQC migration for the LMICs is explored in this work.

It is important to also bear in mind how any security architecture developed will have an effect on real-time data needs. Examples include pandemic surveillance and clinical risk prediction (RPN) or survival risk modeling. The need to detect and understand the spread and impact of Covid-19 across multiple health authorities and regions around the world is one of the most outstanding examples of why effective cybersecurity architecture for health is needed (Ezeogu, 2023). While Zero-Trust and PQC might be proposed in silos, any real-world deployment has to account for access, performance, scalability, and security at the same time. In many cases, that often means difficult design and policy decisions about data privacy, encryption overhead, permission access, and trust management.

This article proposes a roadmap to PQ-ZTA adoption and deployment at the national health system level. The roadmap, framework, and proposed path to adoption are based on recent literature and developments in cryptography, ZTA, secure computation, and health system deployment. In this way, the recommendations and high-level approach proposed by the authors is timely, relevant, and evidence-based, offering important technical and policy insights for national governments, health leaders, IT stakeholders, and security engineers, and those tasked with securing national health systems from internal, external, and future adversaries.

LITERATURE REVIEW

Post-Quantum Cryptography (PQC) for National Health System

Quantum threats to cryptography have instigated a global race for secure quantum-resistant algorithms. Shor’s algorithm, which can efficiently factor large integers, endangers RSA and elliptic curve–based cryptosystems on which most health databases and communication networks rely (Mosca, 2018). In the healthcare context, the vulnerability of national health systems could be fatal by putting medical records, genomic sequences, and clinical trials information at the mercy of adversaries.

A study by Ezeogu (2025a) has recognized PQC as a strategic technology that, when adopted on time, can future-proof health data assets. Lattice-based, code-based, and multivariate polynomial systems have been proposed for electronic health records (EHRs), each with a different footprint on system performance. The early mover advantage, Ezeogu (2025a) argues, is to map national health data assets and define a phased migration plan that leaves room for interoperability with conventional systems.

Privacy-preserving Data Sharing Mechanisms for Health Data89

Sharing of healthcare data poses unique challenges. Unlike financial and transactional data, healthcare data are much more sensitive and personal in nature. Privacy laws in most jurisdictions are quite strict and abiding by policies like HIPAA (United States) and GDPR (European Union) is mandatory for any data sharing initiatives. Traditional data de-identification approaches have also proven to be inadequate, as shown by successful re-identification attacks from cross-reference datasets (Sweeney, 2015).

A significant advancement in the work by Ezeogu (2025b) has been made to this issue using synthetic data generation, which is capable of preserving the privacy of individual records in a dataset and allowing safe data sharing for research and training purposes. Research institutions or countries that want to collaborate also stand to benefit from secure multiparty computation, a process that allows analysts from different servers to perform computations without sharing raw data (Ezeogu & Osigwe, 2025). Similarly, homomorphic encryption allows computations to be carried out on encrypted data, allowing analysts to access information without accessing the data itself (Ezeogu, 2025e). These solutions are quite in line with the Zero-Trust principles of not trusting data and information by default, thereby reducing the need to trust third-party vendors or data custodians.

Security of Big Data Pipelines in Population Health

The increasing demand for big data analytics to mine information on population health has exposed critical vulnerabilities in the data collection, transmission, and processing pipelines. Ezeogu and Emmanuel (2025) had revealed that real-time detection of network traffic anomalies coupled with end-to-end data encryption are indispensable in a big health data scenario. Streams of health data used in tasks like survival risk prediction also call for such architectures to be not only secure but also scalable (Ezeogu, 2023).

Machine and deep learning algorithms are increasingly being used to automate predictive analytics in health, and this has been shown to be a potential attack surface for the extraction of protected patient information or false predictions in clinical settings (Ezeogu, 2025c). Explainable AI (XAI) for Population Health Segmentation was seen to offer the dual benefits of model interpretability and security in Ezeogu (2024). Without these, national health systems are likely to be blind to the illegal harvesting and misuse of their data resources in the guise of research.

Zero-Trust Architectures for Healthcare

Zero-Trust Architecture (ZTA) has been increasingly gaining attention as a viable alternative to traditional cybersecurity approaches. The ZTA principles, formally articulated in Zero Trust Architecture Framework by NIST (Rose et al., 2020), of "never trust, always verify" are especially pertinent in healthcare. Insider threats, third-party vendor access to sensitive information, and the proliferation of mobile and remote devices in healthcare pose complex challenges to healthcare security. ZTA principles of continuous verification of identity and authorization, and strong access control and micro-segmentation of networks can potentially block adversarial lateral movement in systems (Rose et al., 2020).

For healthcare, ZTA can be configured in data-sensitive processes like secure cross-hospital sharing, cloud-hosted EHR systems, and secure telemedicine ecosystems. However, traditional Zero-Trust models have hinged on existing cryptographic primitives that are vulnerable to a quantum adversary. A marriage between PQC and ZTA results in an architecture we coin Post-Quantum Zero-Trust Architecture (PQ-ZTA) that has not only great potential for adoption in the quantum era but in the current landscape as well.

Literature Gaps

While there is plenty of literature on PQC, privacy-preserving computation, and Zero-Trust in healthcare, there is a significant gap in work that looks to bridge all three and design a viable technological and operational roadmap for national health systems. Most studies focus on the constituent elements: cryptography and its security or interoperability, big data security in health, or ZTA pilots, but leave out an end-to-end design. This thesis recognizes these gaps and considers the need for a cohesive strategy that unifies the disparate PQC and ZTA security efforts while factoring the special healthcare constraints of regulatory compliance, cross-border frameworks, real-time analytics, and low-latency responses.

METHODOLOGY

This The methodology for this study is based on a conceptual synthesis and framework development approach, appropriate for fields where technological, regulatory, and organizational domains converge. Rather than testing a hypothesis empirically, the research integrates insights from post-quantum cryptography (PQC), Zero-Trust Architecture (ZTA), and healthcare informatics literature to design a roadmap for secure data sharing in national health systems. The methodology consists of four stages: (1) literature collection and screening, (2) comparative analysis, (3) framework integration, and (4) validation through case mapping.

Literature Collection and Screening

A targeted literature review was conducted to identify sources addressing post-quantum cryptography, zero-trust architectures, privacy-preserving computation, and healthcare data governance. Databases searched included IEEE Xplore, PubMed, Scopus, and Google Scholar. Inclusion criteria emphasized peer-reviewed studies, technical frameworks, and policy documents published between 2015 and 2025. Key sources included:

- Works on PQC and health data security (Ezeogu, 2025a; Mosca, 2018).
- Research on synthetic data generation and SMPC for healthcare collaboration (Ezeogu, 2025b; Ezeogu & Osigwe, 2025).
- Studies on real-time health data analytics and big data pipeline security (Ezeogu, 2023; Ezeogu & Emmanuel, 2025).
- Policy and technical guidelines such as NIST's Zero Trust Architecture framework (Rose et al., 2020).

Exclusion criteria involved duplicate studies, non-peer-reviewed sources (except recognized standards or white papers), and works not directly relevant to healthcare or cybersecurity

Comparative Analysis

The second phase involved a comparative matrix analysis of PQC techniques, privacy-preserving mechanisms, and ZTA implementations. Each method was assessed against four criteria critical to national health systems:

1. Security strength (quantum resistance, resistance to insider threats).
2. Computational performance (latency, scalability for

large datasets).
3. Regulatory compliance (alignment with HIPAA, GDPR, and international cross-border frameworks).
4. Practical feasibility (cost, infrastructure, and adoption barriers for small and large providers).
This comparative analysis highlighted trade-offs between computationally expensive methods (e.g., homomorphic encryption) and more scalable but less robust approaches (e.g., synthetic data).

Framework Integration

Building upon the comparative analysis, the study adopted a design science approach to construct the roadmap for Post-Quantum Zero-Trust Architecture (PQ-ZTA). The roadmap integrates four technological and governance dimensions:

- Cryptographic Migration: Gradual integration of PQC algorithms into existing EHR and health data pipelines (Ezeogu, 2025a).
- Zero-Trust Enforcement: Implementation of continuous authentication, least-privilege access, and micro-segmentation based on NIST guidelines (Rose et al., 2020).
- Privacy-Preserving Collaboration: Incorporation of synthetic data, SMPC, and homomorphic encryption to enable secure research collaboration (Ezeogu, 2025b; Ezeogu & Osigwe, 2025; Ezeogu, 2025e).
- Real-Time Threat Detection: Integration of anomaly detection pipelines for big health data streams (Ezeogu & Emmanuel, 2025).

This integrative approach allows PQC and ZTA to be treated not as parallel solutions but as mutually reinforcing paradigms.

Validation through Case Mapping

To ensure practical relevance, the proposed roadmap was mapped against real-world case contexts, including:

- Pandemic surveillance systems that rely on real-time big health data analytics (Ezeogu, 2023).
- Cross-border research collaborations, where privacy-preserving mechanisms such as SMPC are essential (Ezeogu & Osigwe, 2025).
- National EHR infrastructures, where policy-driven access controls intersect with cryptographic enforcement.

While no empirical testing was performed, this case mapping exercise validates that the roadmap addresses existing vulnerabilities and aligns with the practical needs of national health systems.

Methodological Limitations

This study is limited by its conceptual nature. While the roadmap is informed by state-of-the-art literature and frameworks, empirical testing (e.g., simulation of PQ-ZTA under healthcare workloads) was beyond its scope. Future work should involve pilot implementation studies within healthcare organizations to assess performance trade-offs and identify optimization strategies.

RESULTS AND DISCUSSION

The article synthesized concepts and techniques from post-quantum cryptography (PQC), Zero-Trust Architecture (ZTA), and privacy-preserving computation. This section discusses and describes the final results (roadmap) for enabling national health systems to engineer secure, privacy-preserving, quantum-safe healthcare data-sharing systems. The conceptual framework in Figure 1 was analyzed and applied, and the results are presented below in four phases in the same order that the security, privacy, and governance mechanisms described in the roadmap would be introduced into a national health system's existing healthcare delivery ecosystems.

Phase 1 – Cryptographic Migration to Post-Quantum Standards

The first finding of the research was that the healthcare industry must transition to post-quantum cryptography standards as soon as practical and that RSA and ECC are no longer viable in the post-quantum era (Ezeogu, et al., 2025). As the theoretical and applied underpinnings of PQC are out of scope for this article, we refer the reader to the recent article by NIST (Alagic et al., 2022) for authoritative guidance. The good news is that health systems do not have to "rip and replace" all deployed cryptographic modules because some, such as symmetric ciphers, are naturally PQC-safe. However, as EHRs, telemedicine, and other aspects of E-health are commonly protected by RSA and ECC, national health systems are advised to phase in ZTA protocols based on PQC and have the following strategies ready for immediate and widespread deployment:

- Lattice-based schemes like CRYSTALS-Kyber

- Hash-based signatures like SPHINCS+
- Code-based techniques

In the short term, hybrid approaches are likely to be used to maintain both backward compatibility with existing architectures and agility in cloud-hosted environments. At the very least, it will be recommended that all new applications, modules, and platforms for storing EHRs, genomic data, and clinical images adopt PQC standards. In particular, clinical imaging archives and genomic databases should be transitioned first because they are legacy-encrypted today and need quantum-safe algorithms due to their longevity and sensitivity. The costs of cryptographic migrations at scale can be considerable, but incremental deployment starting with the most mission-critical datasets can be an effective approach (Rose et al., 2020). This is the first major update of the roadmap for post-quantum ZTA, which was published a decade ago as a four-step process (Shahid et al., 2022).

Phase 2 – Zero-Trust Enforcement

The second major result and insight generated from our review and conceptual framework is that ZTA principles are an effective way to enforce cryptographic policies at both the organization and national levels. ZTA has been successfully deployed in numerous enterprise settings, including healthcare infrastructures, to address data integrity and insider threat challenges (Kruse et al., 2017). For example, given the pace of cloud adoption and workforce digitalization in healthcare, there is now much greater risk of insider threats (Shahid et al., 2022). Moreover, ransomware and malicious lateral access have become major problems for healthcare organizations, as cybercriminals realize that EHRs are both highly valuable and vulnerable in most hospitals and clinics (Ahn et al., 2020).

The key to building a Zero-Trust Architecture is that, by definition, no resource, user, or device on the network is trusted implicitly. ZTA is enabled by the principles of continuous verification, least-privilege access, and micro-segmentation enforced dynamically and consistently throughout the system (Rose et al., 2020). For instance, a doctor querying oncology data from a home device must be authenticated by credentials, device posture, geolocation, and behavioral analytics in real time. However, the integration of PQC algorithms into ZTA authentication protocols is recommended as a best practice for hardening healthcare infrastructure against quantum-capable adversaries who will no doubt exploit weaknesses in classical authentication systems.

Phase 3 – Privacy-Preserving Collaboration

The third area of insight and information that the literature review and mapping efforts brought to the fore was that privacy-preserving computation is a set of mechanisms that can enable cross-institutional and international data sharing on a large scale for population health research, pandemic response, or healthcare analytics. Synthetic data, secure multiparty computation (SMPC), and homomorphic encryption have emerged as the leading methods, each with strengths and weaknesses in clinical applications. The central insight from each of these lines of work is that traditional pseudonymization and anonymization have been proven to be ineffective at preserving privacy and enabling citizen trust in health data sharing (Sweeney, 2015). In contrast,

- Synthetic data enables creation of representative research datasets while minimizing exposure (Ezeogu, 2025b).
- SMPC can enable, for example, hospitals across national borders to jointly compute risk scores for cancer data without direct exchange of raw patient data (Ezeogu & Osigwe, 2025).
- Homomorphic encryption enables encrypted computation in outsourced cloud environments, making it possible for, say, national health agencies to perform sophisticated population health studies while data remains confidential (Ezeogu, 2025e).

Results from recent studies of these methods show that they not only increase the trustworthiness of healthcare organizations with respect to regulatory compliance (GDPR, HIPAA) but also that citizens are more willing to grant data access when privacy-preserving computation is demonstrated. The major drawbacks are the computational overhead of SMPC and homomorphic encryption, which may be prohibitive in time-critical healthcare workflows like triage or patient monitoring (Ezeogu, 2025e). These results and insights are then woven into the overall roadmap for ZTA by noting that privacy-preserving collaboration represents a logical extension of Zero-Trust principles into the space of inter-organizational collaboration and federated analytics.

4.4 Phase 4 – Real-Time Threat Detection and Adaptive Analytics

The final result from the systematic mapping and synthesis processes was that real-time monitoring, anomaly detection, and adaptive analytics are essential to creating a ZTA that is useful for the task of keeping national health systems safe in a rapidly changing and complex threat landscape. Clinical data, workflows, and patient monitoring in modern healthcare organizations increasingly rely on streaming data pipelines and automated EHR processing for critical functions like survival risk prediction, epidemic tracking, and intensive care monitoring (Ezeogu, 2023). A real-time failure to ingest data, a DoS attack, or a ransomware incident can endanger lives.
Ezeogu and Emmanuel (2025) point out the need for online anomaly detection and response that can be grafted onto big health data systems and platforms. These include machine learning-based anomaly detection models that are trained on baseline access and query behavior and can flag suspicious or anomalous behavior, including brute force credential stuffing, lateral movement, or unusual data requests. The use of explainable AI can also ensure that, for instance, chief information security officers (CISOs) are able to follow the logic behind automated AI threat detection and response actions (Ezeogu, 2024). These results and insights are then incorporated into the ZTA roadmap by noting that continuous monitoring and early threat detection is an orthogonal concern that overlaps all the previous three aspects.

Cross-Phase Synergies

As we can see in Figure 4, while the four phases can be discussed and analyzed separately, there are important cross-phase synergies. Cryptographic migration underlies zero-trust enforcement, privacy-preserving collaboration extends zero-trust principles to inter-organizational contexts, and real-time anomaly detection ensures that critical vulnerabilities in all earlier steps can be exposed and addressed quickly. When taken together, these results form a coherent PQ-ZTA model for national health systems.

Practical Challenges

There are several practical challenges to ZTA deployment in healthcare:

• Cost and performance: Implementing ZTA and PQC can be expensive and resource-intensive, particularly for smaller healthcare providers (Shahid et al., 2022).
• Regulatory hurdles: Data sharing across borders is complex and requires alignment of GDPR, HIPAA, and other regulatory frameworks, which is politically challenging (Ezeogu & Osigwe, 2025).
• Performance trade-offs: Post-quantum and privacy-preserving algorithms (e.g., PQC, SMPC, homomorphic encryption) are computationally intensive, potentially impacting real-time data processing required for certain clinical decisions (Ezeogu, 2025).

These results are somewhat disconcerting, as they point to significant obstacles to the ZTA roadmap as it currently stands. As such, further research into case studies, simulation models, and pilot deployments will be needed to confirm the feasibility of PQ-ZTA. We recommend that select hospitals or research consortia volunteer to serve as testbeds for future pilots of these approaches.

Strategic Implications

The strategic implications of this work, its outcomes and findings, and the entire research area for healthcare decision-makers, policymakers, system leaders, and other stakeholders are significant for the following reasons:

1. Future-proof security: PQC migration will protect the confidentiality and integrity of patient data against classical and quantum threats.
2. Trust and public confidence: By adopting privacy-preserving computation, health authorities will build trust with the citizenry and the general public, which is key to broader health data access for medical research and digital health.
3. Collaboration and innovation in health: A PQ-ZTA will enable secure data sharing both within national health systems and cross-border with researchers and other health systems for population health, pandemic preparedness, and medical research.
4. Policy leadership: Governments can use PQ-ZTA as a means to drive technical innovation, interoperability, and adherence to regulatory mandates.

CONCLUSION

In summary, this article has attempted to build a roadmap for the implementation of a post-quantum

Zero-Trust Architecture (PQ-ZTA) that is scalable, privacy-preserving, regulation-compliant, and also resilient against classical and quantum threats. The evidence that supports the case for ZTA in healthcare (Kruse et al., 2017) shows that, without Zero-Trust principles of identity and device posture verification, micro-segmentation, and least-privilege access (Rose et al., 2020), the integrity, confidentiality, and availability of EHRs and other mission-critical healthcare information are under constant threat. However, the evidence is also conclusive that ZTA must be coupled with PQC and privacy-preserving computation if health systems are to remain resilient into the future against quantum and increasingly AI-driven and automated attacks (Mosca, 2018).

The roadmap presented in the main body of the paper, which was tested, validated, and corroborated with the existing literature and our conceptual mapping, is based on four phases in the order that PQ-ZTA mechanisms are likely to be introduced into healthcare infrastructures:

1. Migration of cryptographic systems to PQC algorithms and protocols. This will be necessary to future-proof healthcare security, as RSA and ECC are vulnerable to quantum computers in a few years (Mosca, 2018).
2. Zero-trust enforcement using continuous verification, least-privilege access, and network micro-segmentation. The roadmap for achieving ZTA was outlined and tested in earlier work (Shahid et al., 2022) and will have to be updated to be specific to national health systems.
3. Privacy-preserving computation using synthetic data, SMPC, and homomorphic encryption to scale data sharing, support regulatory compliance with privacy laws such as GDPR and HIPAA, and foster citizen trust. The growing body of literature on these techniques shows their promise and potential limitations, so any practical testbed or implementation will need to take these results into account (Ezeogu, 2025b; Ezeogu & Osigwe, 2025; Ezeogu, 2025e).
4. Real-time threat detection and adaptive analytics based on streaming data ingestion, online anomaly detection, and explainable AI to maintain high security postures. The new research programs that our team has developed to address these needs have shown that most current systems lack the critical response component, though algorithms for many important medical and health data use cases have been successfully demonstrated (Ezeogu & Emmanuel, 2025).

Limitations of the proposed roadmap include a high cost of cryptographic migrations, performance penalties from privacy-preserving computation, a complex regulatory environment, and a possible deficit of technical talent in healthcare (Shahid et al., 2022). These limitations point to avenues for future research, including both theoretical improvements to PQC, privacy-preserving algorithms for specific healthcare applications, and empirical case studies of PQ-ZTA testbeds. In this way, the academic community and industry can work together to realize the promise and vision for PQ-ZTA outlined here.

Practical takeaways from this work for healthcare CIOs, health system leaders, and policymakers, among others, are that they have a unique opportunity to demonstrate global leadership and policy innovation by aligning the technical architecture and infrastructure of national health systems with Zero-Trust, PQC, and privacy-preserving computation as a practical means to three strategic imperatives. These are future-proofing health data against quantum, insider, and advanced external threats, building trust and confidence with the citizenry and the public through privacy-preserving computation, and innovating in health research, discovery, and collaboration by scaling secure and interoperable data sharing with domestic and international partners.

REFERENCES

1. Alagic, G., Alperin-Sheriff, J., Cooper, D., Dang, Q., Kelsey, J., Liu, Y. K., … & Moody, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process. *NIST Interagency/Internal Report (NISTIR) 8413*. https://doi.org/10.6028/NIST.IR.8413

2. Adekunle, K. A. (2025). Operational Efficiency Meets Safety: Leveraging Industrial Management Principles to Strengthen EHS Performance. *Multidisciplinary Journal of Healthcare (MJH), 2*(1), 114-144.

3. Adekunle, K. (2024). Empowering Communities for a Greener Future: The Role of Public Awareness and Engagement in Sustainable Waste Management.

4. Adekunle, K. (2024). Technological Innovations in Industrial Waste Recycling. *Available at SSRN 4874176*.

5. Ezeogu, A. O. (2025). POST-QUANTUM CRYPTOGRAPHY FOR HEALTHCARE: FUTURE-PROOFING POPULATION HEALTH DATABASES AGAINST QUANTUM COMPUTING THREATS. *Research Corridor Journal of Engineering Science*, *2*(1), 29-56.

6. Ezeogu, A. O. (2025). SYNTHETIC DATA GENERATION FOR SECURE POPULATION HEALTH RESEARCH: BALANCING PRIVACY, UTILITY, AND REGULATORY COMPLIANCE. *Multidisciplinary Journal of Healthcare (MJH)*, *2*(1), 51-92.

7. Ezeogu, A. O., & Osigwe, D. F. (2025). Secure Multiparty Computation for Cross-Border Population Health Research: A Framework for International Healthcare Collaboration. *NextGen Research*, *1*(1), 14-39. https://nextgresearch.com/index.php/nextgr/article/view/16

8. Ezeogu, A. O., & Emmanuel, A. (2025). Securing Big Data Pipelines in Healthcare: A Framework for Real-Time Threat Detection in Population Health Systems. *Research Corridor Journal of Engineering Science*, *2*(1), 8-28.

9. Ezeogu, A. O. (2025). Homomorphic Encryption in Healthcare Analytics: Enabling Secure Cloud-Based Population Health Computations. *Journal of Advanced Research*, *1*(02), 42-60.

10. Ezeogu, A. O. (2023). Real-Time Survival Risk Prediction with Streaming Big Health Data: A Scalable Architecture. *Contemporary Journal of Social Science Review*, *1*(1), 50-65. https://doi.org/10.63878/cjssr.v1i1.123

11. Ezeogu, A. O. (2024). Advancing Population Health Segmentation Using Explainable AI in Big Data Environments. *Research Corridor Journal of Engineering Science*, *1*(1), 267-2883.

12. Ezeogu, A. (2025). Data Analytics Approach to Population Health Segmentation. *Multidisciplinary Journal of Healthcare (MJH)*, *2*(1), 93-113.

13. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263

14. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38–41. https://doi.org/10.1109/MSEC.2018.2888786

15. M'Bachi, F. D. N. C. (2025). Diaspora and Afro-Descendants in Angola–USA Business Relations. *MULTIDISCIPLINARY JOURNAL OF INSTRUCTION (MDJI)*, *8*(1), 1-20.

16. M'Bachi, F. D. N. C. (2025). Strengthening Angola-USA Relations: A Win-Win Perspective. *Journal of Social Sciences and Community Support*, *2*(1), 57-68.

17. M'Bachi, F. D. N. C. (2025). Lobito Corridor's Impact on Angola-USA Trade Relations. *MULTIDISCIPLINARY JOURNAL OF INSTRUCTION (MDJI)*, *8*(1), 21-25.

18. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

19. Shahid, M., Ahmad, R. W., Javaid, N., Afzal, M. K., & Alrajeh, N. A. (2022). Zero trust security in healthcare: State-of-the-art, challenges, and future research directions. *IEEE Access*, *10*, 51142-51160. https://doi.org/10.1109/ACCESS.2022.3171555

20. Sweeney, L. (2015). Only you, your doctor, and many others may know. *Technology Science*, *2015092903*, 1–25.