



Review Article

Quantum-Secure Healthcare: A Comprehensive Review of Post-Quantum Cryptography and Cyber Defense in IoMT

Ateeq Ur Rehman Butt¹, Muhammad Asif², Muhammad Atif Rasheed^{3*} and Sumaira Shafiq⁴

¹Department of Computer Science, University of Kamalia, Kamalia, Pakistan

²Department of Computer Science, National Textile University, Faisalabad, Pakistan

³Department at UofT: Business Transformation and Program Management University of Toronto, Canada.

⁴Department of Computer Science, University of Poonch Rawalakot, Azad Kashmir, Pakistan

*Corresponding Author Email: mrasheed@utoronto.ca

<https://orcid.org/0009-0009-7009-662X>

Received: 14/03/2026; Revised: 30/04/2026; Accepted: 25/05/2026; Published: 01/06/2026

<https://doi.org/10.65278/IJTACI.2026.67>

Abstract: The increasing digitalization of the healthcare system, driven by the use of electronic health records, medical IoT devices, and AI-aided diagnostics, has significantly expanded the attack surface for cyber threats. Even though current cryptographic protocols provide sufficient security against classical adversaries, new developments in quantum computing threaten the confidentiality, integrity, and availability of medical information as never before. Shor's and Grover's quantum algorithms could breach extensive asymmetric and symmetric encryption systems, rendering modern healthcare security systems obsolete. This review consists of an in-depth and organized analysis of the dynamic quantum threat environment in the context of healthcare ecosystems and the need to move towards quantum-resilient security architectures. The review provides a synthesis of the existing literature on post-quantum cryptography (PQC), noting lattice-based, hash-based, multivariate, and code-based algorithms as potentially viable long-term replacements for cryptography. Moreover, we examined the cybersecurity issues associated with quantum-enabled attacks of medical IoT systems, clinical decision-support systems, wearable sensors, telemedicine systems, and cloud-based health information exchanges. Another aspect of quantum-classical defense mechanisms examined in review is hybrid quantum-classical defenses, quantum key distribution (QKD), quantum random number generation (QRNG), and blockchain-based trust systems aimed at making



systems resilient to advanced persistent quantum attacks. This paper identifies key gaps and outlines future research directions for developing quantum-secure medical systems, quantum computation, and healthcare cybersecurity. The results highlight the importance of early implementation of PQC standards and a layered cyber defense approach to protect patient privacy, ensure regulatory compliance, and retain trust in next-generation digital medical data communication.

Keywords: Quantum Computing; Health Informatics; IoMT; Cryptography; Cyber Defense

1. Introduction

The healthcare sector is undergoing a digital transformation, increasingly relying on technologies such as electronic health records (EHRs), the Internet of Medical Things (IoMT), telemedicine, and AI-driven diagnostic tools. While these advancements have led to improved patient care, they also expose the sector to heightened cybersecurity risks [1]. Traditional cryptographic systems, which have been used to protect sensitive medical data, are now facing significant threats from the rapid progress of quantum computing. This introduction outlines the growing challenges in securing healthcare systems against quantum threats, reviews the limitations of existing research in this domain, and highlights the objectives and novel contributions of this study.

1.1 Background and Growing Cybersecurity Threats in Healthcare

The integration of digital systems in healthcare has revolutionized the way patient information is managed, leading to substantial improvements in treatment accuracy and overall care. The widespread use of IoMT devices, coupled with cloud-based health data exchanges and AI-based decision support systems, has introduced new vulnerabilities [2]. These digital platforms are particularly susceptible to cyberattacks, making the need for robust cybersecurity protocols more critical than ever. With the emergence of quantum computing, the very foundations of modern cryptography are being questioned. Quantum computers, when fully realized, will be capable of executing algorithms that can break widely used cryptographic protocols, such as RSA and ECC, within a practical time frame. Shor's algorithm, for instance, can efficiently factor large numbers, undermining the security of asymmetric encryption. Similarly, Grover's algorithm poses a threat to symmetric encryption by providing a quadratic speedup in brute-force search processes [3]. As the healthcare sector continues to digitize, these vulnerabilities are compounded by the increasing sophistication of cyberattacks, further escalating the risks to patient data confidentiality and the integrity of medical systems. Therefore, it is imperative to explore solutions that can withstand both current and quantum-enabled cyber threats.

1.2 Limitations of Previous Studies

While the threat posed by quantum computing to healthcare systems has been recognized, the body of research addressing post-quantum cryptography (PQC) in the healthcare context is still in its nascent stages. Several studies have explored the potential of PQC algorithms in general, but only a few have focused on the specific needs and challenges of healthcare applications. Furthermore, many existing studies provide theoretical models or simulations, which often overlook the practical, real-world complexities of implementing quantum-safe technologies in a sector as critical and dynamic as healthcare [4]. Additionally, previous research has largely concentrated on the theoretical aspects of quantum computing's impact on

cryptography, leaving gaps in terms of the integration of hybrid quantum-classical defense mechanisms. The combination of quantum and classical systems in a multi-layered defense structure remains underexplored, particularly in the context of healthcare IoMT devices, telemedicine systems, and cloud-based health information exchanges. Another limitation of existing studies is the lack of consideration of regulatory frameworks and ethical implications, such as patient privacy concerns and data governance in a quantum-enabled world. While post-quantum cryptography offers strong security promises, its real-world applicability must be carefully evaluated in the light of compliance requirements like HIPAA, GDPR, and other regional data protection laws [5].

A notable limitation in existing review literature is the lack of detailed analysis of healthcare-specific implementation challenges associated with post-quantum cryptographic adoption. As an example, the limitations of computational overhead, memory, and energy efficiency on resource-limited medical IoMT devices are frequently ignored in previous research and can profoundly impact the viability of deploying PQC algorithms. There is also little focus on interoperability issues in heterogeneous healthcare systems, that is, spanning hospitals, cloud systems, wearables, and legacy medical infrastructure, which are seldom studied in detail, although they are essential to real-world implementation. The other key gap is the fact that little has been done to explore the idea of hybrid quantum-classical defense. Although in some studies, the concept of hybrid approaches is recognized, the questions concerning the architectural design, integration strategies, and scalability issues in healthcare settings are often overlooked. Also, little attention has been paid to pragmatic evaluation frameworks, which evaluate the effectiveness and security trade-offs of these hybrid solutions under realistic healthcare workloads. These gaps must be addressed to overcome the gap between theoretical cryptographic developments and their practical application in secure healthcare systems [6, 7].

1.3 Objectives of the Study

This study aims to fill the existing gaps in the literature by offering a comprehensive review of the quantum security landscape in healthcare systems. The key objectives of this study are:

- To examine the vulnerabilities of current cryptographic protocols in the face of quantum computing and analyze their potential failure points in healthcare systems.
- To provide a detailed analysis of post-quantum cryptographic algorithms, including lattice-based, hash-based, multivariate, and code-based methods, with a focus on their suitability for protecting medical data in the long term.
- To investigate quantum-enhanced defense mechanisms such as Quantum Key Distribution (QKD), Quantum Random Number Generation (QRNG), and hybrid quantum-classical defense strategies, evaluating their potential to safeguard healthcare infrastructure against quantum-enabled threats. To evaluate the security challenges posed by quantum attacks to IoMT devices, clinical decision-support systems, wearable sensors, and telemedicine platforms, and suggest practical defense strategies tailored to the healthcare sector.
- To analyze the ethical, regulatory, and practical considerations involved in implementing quantum-secure systems in healthcare, with a focus on compliance with healthcare data protection regulations and fostering patient trust.

1.4 Main Contributions

This study makes several novel contributions to the field of quantum-resilient cybersecurity in healthcare systems:

- In-depth review of PQC algorithms in the context of healthcare, focusing not only on theoretical aspects but also on practical challenges and implications for integration into real-world healthcare environments.
- Exploration of hybrid defense mechanisms that combine quantum and classical approaches to safeguard medical data, an area that has received limited attention in previous research.
- Practical analysis of quantum-enhanced technologies like QKD and QRNG, assessing their feasibility and potential to mitigate quantum threats in healthcare infrastructure.
- Insight into regulatory and ethical challenges in the adoption of quantum-secure technologies within healthcare systems, contributing to the broader discussion on how to ensure secure and compliant transitions to quantum-safe environments.
- A roadmap for future research in the domain, identifying key areas where further development and innovation are needed to create truly quantum-secure healthcare systems.

This paper is organized as follows: Section 2 provides a detailed overview of quantum computing and its implications for cryptographic systems, with a particular focus on healthcare applications. Section 3 reviews the existing literature on post-quantum cryptography, including an analysis of PQC algorithms that could potentially replace classical cryptosystems in healthcare settings. Section 4 examines the cybersecurity risks posed by quantum-enabled attacks on IoMT devices, clinical decision-support systems, wearable sensors, and health information exchanges. Section 5 discusses quantum-enhanced defense mechanisms, including QKD, QRNG, and hybrid quantum-classical defenses, and evaluates their suitability for healthcare applications. Section 6 focuses on the regulatory, ethical, and practical considerations of adopting quantum-secure technologies in healthcare, with recommendations for policymakers, healthcare providers, and researchers. Section 7 concludes with a summary of the findings, outlines the study's contributions, and suggests avenues for future research in developing quantum-secure healthcare systems.

2. Quantum computing and cryptographic foundations

This section provides the technical foundation necessary to understand how quantum computing alters the security assumptions of modern cryptographic systems. By outlining the core principles of quantum computation and analyzing quantum algorithms relevant to cryptography, this section establishes a threat model that is particularly critical for long-term healthcare data protection.

2.1 Fundamentals of Quantum Computing

Quantum computing is based on the principles of quantum mechanics, which fundamentally differ from classical computing paradigms. Unlike classical bits that exist strictly in binary states of 0 or 1, quantum computers operate on qubits, which can exist in a superposition of states. This property enables quantum systems to process a vast number of computational possibilities simultaneously. Superposition, combined with quantum interference, allows quantum algorithms to amplify correct solutions while suppressing incorrect ones. Another defining feature of quantum computing is quantum entanglement, a phenomenon where the state of one qubit is intrinsically linked to the state of another, regardless of physical distance. Entanglement enables coordinated operations across multiple qubits and plays a central role in achieving exponential computational advantages over classical systems. Together, superposition and entanglement

enable quantum parallelism, which underpins the efficiency of quantum algorithms that outperform their classical counterparts [8]. Current quantum hardware exists in the so-called Noisy Intermediate-Scale Quantum (NISQ) era, in which quantum systems have few qubits and are vulnerable to environmental noise. In spite of the fact that current quantum computers are not yet capable of breaking large-scale cryptography systems, quantum error correction, qubit coherence, and scalable architectures are rapidly progressing, which means that cryptographically relevant quantum machines can be achieved in the not too distant future. This projected development makes it important that the data-intensive industries like healthcare are given security planning at an early stage.

2.2 Quantum Algorithms Relevant to Cryptography

The cryptographic threat posed by quantum computing primarily stems from specific algorithms that offer substantial speedups over classical approaches. Among these, Shor's algorithm represents the most significant risk to public-key cryptography. It enables polynomial-time solutions to integer factorization and discrete logarithm problems, which form the security basis of RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC). Once scalable quantum computers are realized, these widely deployed schemes would become computationally insecure [9]. Grover's algorithm presents a different, yet equally important, challenge. It provides a quadratic speedup for unstructured search problems, including brute-force key search against symmetric encryption and hash functions. While Grover's algorithm does not completely break symmetric cryptography, it effectively halves the security strength of symmetric keys. This means that a cryptographic system based on symmetric primitives will have to expand key sizes to achieve the same level of security in a quantum adversarial model. Other than the algorithms developed by Shor, Grover, etc., there are still more quantum algorithms under study which can continue to undermine cryptographic constructions. Even though most of these algorithms are still theoretical, their possible effect justifies the necessity of reevaluating cryptographic assumptions in all spheres, in which long-term data confidentiality is essential.

2.3 Implications for Classical Cryptographic Systems

The advent of quantum computing fundamentally challenges the security guarantees provided by classical cryptographic systems. Asymmetric cryptography is particularly vulnerable, as its underlying mathematical problems become tractable under quantum computation. This vulnerability directly affects key exchange, digital signatures, and authentication mechanisms that are critical for secure communication in healthcare infrastructures. Symmetric cryptographic primitives, including block ciphers and cryptographic hash functions, are comparatively more resilient but still experience reduced security margins. The effective weakening of symmetric schemes necessitates modifications in key management strategies and system designs to ensure continued robustness against quantum-enabled adversaries [10]. These cryptographic disruptions have cascading effects on complex digital ecosystems. Healthcare systems, which depend on layered security architectures involving authentication, access control, data encryption, and secure communication channels, face systemic risks if any cryptographic component becomes compromised. Consequently, a partial or delayed response to quantum threats could undermine the overall trustworthiness of healthcare information systems.

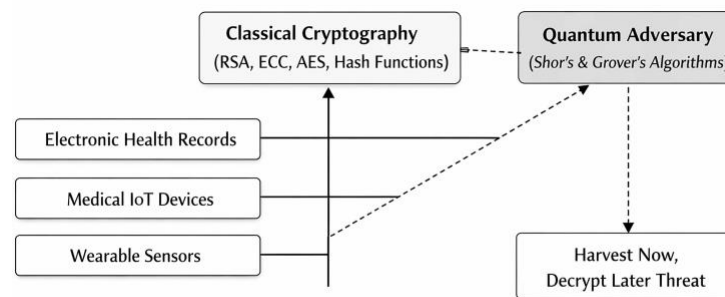
2.4 Quantum Threat Model in Healthcare Environments

Healthcare data presents a uniquely attractive target for quantum-enabled attacks due to its long-term sensitivity and high economic value. Medical records, diagnostic images, and genomic information often

require confidentiality guarantees spanning decades. This temporal dimension introduces the risk of so-called harvest-now, decrypt-later attacks, where adversaries collect encrypted data today with the intention of decrypting it once quantum capabilities mature. The distributed nature of healthcare ecosystems further amplifies this threat. Data flows across hospitals, research institutions, insurance providers, wearable devices, and cloud-based platforms, creating multiple points of exposure. Even if quantum computers are not immediately available, encrypted healthcare data intercepted today may become vulnerable in the future, potentially compromising patient privacy retroactively [8]. Additionally, the increasing reliance on remote healthcare services and interconnected medical devices expands the attack surface. Quantum-enabled adversaries could exploit cryptographic weaknesses to undermine authentication protocols, disrupt secure communications, or manipulate data integrity, posing both privacy and patient safety risks.

2.5 Security Transition Challenges and Readiness

Transitioning from classical cryptography to quantum-resistant security frameworks presents substantial technical and organizational challenges. Healthcare systems often operate on legacy infrastructure with limited flexibility for cryptographic upgrades. Interoperability requirements, regulatory constraints, and performance limitations further complicate the adoption of new cryptographic primitives. Moreover, cryptographic transitions must be executed carefully to avoid introducing new vulnerabilities during migration. Hybrid approaches, where classical and quantum-resistant mechanisms coexist, are likely to play a critical role during this transitional period. Preparing healthcare systems for such transitions requires a comprehensive understanding of both quantum threats and the limitations of existing defenses [11]. Figure 1 presents a conceptual quantum threat model illustrating how advances in quantum computing undermine classical cryptographic protections across interconnected healthcare systems. The figure highlights how quantum-enabled adversaries can compromise classical encryption mechanisms protecting electronic health records, medical IoT devices, cloud-based health platforms, and long-term sensitive medical data



Quantum Threat Model in Healthcare Ecosystems

Figure 1: Quantum threat model illustrating the impact of quantum computing on cryptographic protections within healthcare ecosystems.

3. Post-quantum cryptography for healthcare systems

The cryptographic vulnerabilities introduced by quantum computing have motivated the development of post-quantum cryptography (PQC), a class of cryptographic algorithms designed to remain secure against both classical and quantum adversaries. Unlike quantum-based security solutions that rely on specialized hardware, PQC focuses on software-compatible cryptographic constructions that can be deployed on existing digital infrastructures. This property makes PQC particularly attractive for healthcare systems, which often operate under strict budgetary, regulatory, and interoperability constraints. As healthcare data

requires long-term confidentiality and integrity, the transition to quantum-resistant cryptographic mechanisms has become a strategic priority rather than a theoretical concern. Post-quantum cryptographic algorithms are constructed on mathematical problems that are currently believed to be resistant to quantum attacks. Among the most extensively studied approaches are lattice-based, code-based, hash-based, and multivariate polynomial cryptographic schemes. Lattice-based cryptography has emerged as a leading candidate due to its strong security assumptions and versatility across encryption, digital signatures, and key encapsulation mechanisms [12].

Its security is grounded in hard lattice problems such as the Learning with Errors (LWE) and Shortest Vector Problem (SVP), for which no efficient quantum algorithms are known. These properties make lattice-based schemes suitable for securing data exchanges in healthcare environments that involve frequent authentication and encrypted communication [13, 14]. Another quantum-resistant cryptography is hash-based cryptography, especially a digital signature implementation. They are based on the preimage and collision resistance of cryptographic hash functions and provide provable security assurances even in the quantum adversary case. Although hash-based signatures are computationally efficient and well understood, their practical use is limited by very large signature sizes and key-reuse (state management) issues in healthcare systems, particularly in resource-constrained medical devices. However, their high level of assurance makes them suitable where strong guarantees are needed, such as validating the authenticity of medical records or demonstrating regulatory compliance. Code-based cryptography is based on the hardness of decoding random linear codes, which has resisted both classical and quantum attacks for decades. Such schemes are characterized by extensive history of cryptanalytic analysis, and high security margins. However, their relatively large public key sizes pose challenges for deployment in bandwidth-sensitive healthcare networks, such as remote monitoring systems and mobile health platforms. Despite these limitations, code-based cryptography remains a viable option for backend healthcare infrastructures where storage and transmission overheads are less restrictive [10, 15].

Multivariate polynomial cryptography is based on the difficulty of solving systems of multivariate quadratic equations over finite fields. These schemes offer fast computation and compact signatures, making them appealing for latency-sensitive healthcare applications. However, several proposed multivariate schemes have been broken over time, highlighting the need for cautious evaluation before large-scale deployment. This fragility underscores the importance of continuous cryptanalysis and conservative adoption strategies within safety-critical domains such as healthcare. Regarding a practical deployment of a healthcare perspective, the appropriateness of various post-quantum cryptographic schemes can vary greatly in terms of system constraints and application requirements. Lattice-based cryptography has a good fit for cloud-based EHRs and secure data exchange due to its high security assurance and moderate computational efficiency, though its key sizes can be problematic with lightweight devices [5]. Although they provide high security assurance, hash-based schemes are more suitable in applications with strong security requirements, such as authentication of medical records, but may not be as efficient in high key traffic in a low-resource environment. Code-based cryptography, with large key sizes and fast encryption and decryption speeds, is more appropriate to backend healthcare infrastructures where storage and bandwidth need not be as restrictive. By contrast, multivariate schemes are fast, have compact signatures, and are attractive to latency-sensitive applications such as wearable devices and real-time monitoring systems, but the long-term security stability of these schemes must be taken into consideration. Figure 2 summarizes the taxonomy of post-quantum cryptographic approaches and highlights their relative suitability for healthcare applications involving encryption, digital signatures, and key exchange.

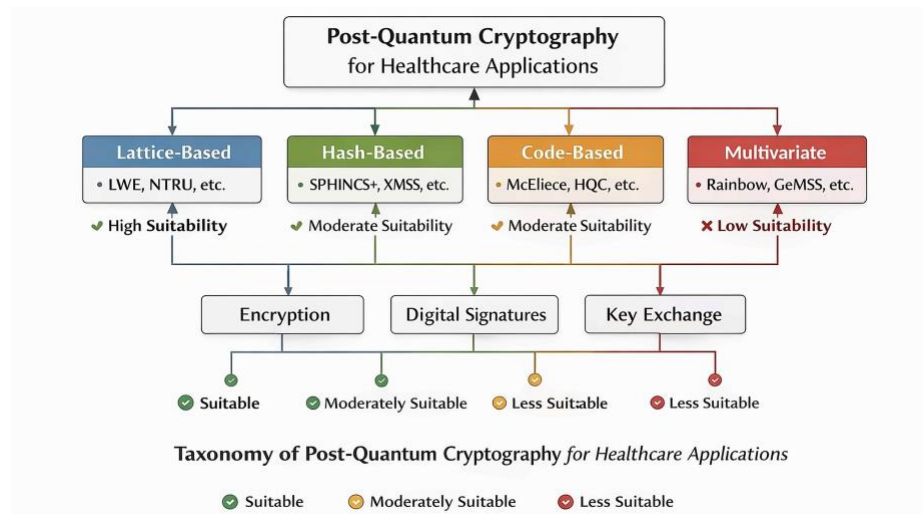


Figure 2: Taxonomy of post-quantum cryptographic approaches for healthcare applications.

The figure 2 categorizes lattice-based, hash-based, code-based, and multivariate schemes and illustrates their applicability to encryption, digital signatures, and key exchange within healthcare systems. Standardization is central to the adoption of PQC across healthcare systems. International initiatives, most notably led by the National Institute of Standards and Technology (NIST), aim to identify and standardize quantum-resistant algorithms suitable for widespread deployment. These efforts consider not only cryptographic security but also implementation efficiency, scalability, and resilience against side-channel attacks. For healthcare organizations, adherence to standardized PQC algorithms is essential to ensure interoperability across institutions, vendors, and regulatory jurisdictions [16, 17].

The integration of PQC into healthcare systems presents several practical challenges. Legacy medical devices, long software update cycles, and strict certification requirements complicate cryptographic migration. Moreover, healthcare environments often consist of heterogeneous systems with varying computational capabilities, ranging from cloud-based analytics platforms to low-power wearable sensors. Selecting PQC schemes that balance security strength with performance and resource efficiency is therefore a nontrivial task. Hybrid cryptographic deployments, in which classical and post-quantum algorithms coexist during a transition period, are increasingly viewed as a pragmatic approach to mitigate migration risks. From a risk management perspective, the adoption of PQC is not solely a technical decision but also a strategic investment in long-term data protection. Healthcare data breaches can have irreversible consequences due to the immutability of medical and biometric information. Consequently, delaying the transition to quantum-resistant cryptography may expose healthcare systems to future retrospective attacks, even if current security measures appear sufficient. Proactive adoption of PQC enables healthcare organizations to future-proof their security architectures while maintaining compliance with evolving data protection regulations [18].

4. Quantum-enabled cybersecurity threats in healthcare systems

The increasing reliance on interconnected digital technologies has fundamentally reshaped healthcare delivery while simultaneously introducing complex cybersecurity challenges. In the context of quantum

computing, these challenges are further amplified as cryptographic safeguards underpinning healthcare infrastructures become vulnerable to quantum-enabled adversaries. Unlike conventional cyber threats, quantum-enabled attacks possess the potential to compromise long-term data confidentiality, disrupt system integrity, and undermine trust across healthcare ecosystems [18]. This section examines how quantum-era threats manifest across critical healthcare technologies and highlights the systemic risks posed to modern medical systems.

Medical Internet of Things (IoMT) devices represent one of the most vulnerable components of healthcare infrastructure. These devices, including implantable sensors, infusion pumps, and remote monitoring tools, often operate under strict resource constraints and rely on lightweight cryptographic mechanisms. Quantum-enabled adversaries could exploit weakened authentication and key exchange protocols to gain unauthorized access, manipulate sensor data, or disrupt device functionality. Such compromises may not only violate patient privacy but also pose direct risks to patient safety by altering clinical readings or device behavior. Figure 3 conceptually illustrates how quantum-enabled threats propagate across interconnected healthcare components, with IoMT devices forming a primary attack entry point [19].

Consider, for example, a remote telemedicine visit in which a patient discloses sensitive diagnostic data to a physician via an encrypted video platform. A hostile party might intercept and store the encrypted session information without instantly decrypting it. As the capability of quantum computing becomes available in the future, the attacker can later decrypt the communication recorded, revealing confidential patient information, medical history, and prescribed treatments. Such harvest-now, decrypt-later scenarios underscore the long-term privacy risks in telemedicine systems with quantum-enabled threats. Telemedicine platforms have emerged as essential healthcare delivery mechanisms, particularly in remote and underserved regions. These platforms depend heavily on secure communication channels for real-time consultations, diagnostics, and prescription services. Quantum attacks targeting cryptographic protocols could enable eavesdropping, session hijacking, or impersonation attacks, thereby exposing sensitive patient-physician interactions. The long-term storage of encrypted telemedicine session data further exacerbates the risk, as intercepted communications may be decrypted retrospectively once quantum computing capabilities mature [20].

Cloud-based electronic health record (EHR) systems constitute another high-value target for quantum-enabled adversaries. These systems aggregate vast volumes of sensitive patient data and support interoperability across healthcare providers, insurers, and research institutions. The centralized nature of cloud infrastructures increases the potential impact of cryptographic compromise. A successful quantum attack on encryption or digital signature mechanisms could enable large-scale data breaches, unauthorized data modification, or denial-of-service attacks. The risk is compounded by the long data retention periods typical of healthcare records, which make them particularly susceptible to harvest-now, decrypt-later strategies [21].

Clinical decision-support systems (CDSS), increasingly augmented by artificial intelligence and machine learning, rely on data integrity and authenticity to generate accurate diagnostic and treatment recommendations. Quantum-enabled attacks targeting cryptographic verification mechanisms could result in data poisoning or manipulation of clinical models. Such attacks may lead to incorrect diagnoses, inappropriate treatment decisions, or erosion of clinician trust in automated systems. The cascading effects of compromised CDSS highlight the broader implications of quantum threats beyond data confidentiality, extending into clinical reliability and patient outcomes.

Wearable health technologies and remote patient monitoring platforms further expand the healthcare attack surface. These systems continuously collect physiological data and transmit it to centralized analytics platforms for assessment. Weak cryptographic protections combined with quantum-enabled attacks could allow adversaries to intercept, alter, or fabricate health data streams. The implications extend beyond privacy concerns, as falsified or corrupted data may trigger unnecessary medical interventions or conceal critical health conditions.

Table 1 provides a comparative overview of key healthcare technologies, associated quantum-enabled threats, and their potential impact. This synthesis highlights the diversity of attack vectors and underscores the need for tailored security strategies across different healthcare domains.

Beyond individual technologies, quantum-enabled threats introduce systemic challenges for healthcare ecosystems. Interoperability requirements necessitate data sharing across organizational boundaries, increasing exposure to cryptographic weaknesses. Furthermore, healthcare environments often integrate legacy systems with modern platforms, creating heterogeneous security postures that are difficult to uniformly upgrade. These factors collectively heighten the risk of cascading failures, where compromise of one component undermines the security of interconnected systems [22]. Figure 3 visually summarizes the primary quantum-enabled attack surfaces within healthcare infrastructures and highlights how vulnerabilities in one domain can propagate across the ecosystem. Such visual synthesis reinforces the need for holistic threat modeling that accounts for both technological interdependencies and evolving adversarial capabilities.

5. Quantum-enhanced and hybrid cyber defense mechanisms for healthcare

The emergence of quantum-enabled cyber threats necessitates a fundamental shift from isolated security controls toward comprehensive, layered defense architectures. In healthcare environments, where patient safety, data integrity, and regulatory compliance are tightly coupled, reliance on a single cryptographic solution is insufficient. Instead, quantum-resilient healthcare security requires the integration of post-quantum cryptography with quantum-enhanced technologies and hybrid defense strategies that collectively address confidentiality, integrity, and availability across diverse system components. Figure 3 illustrates how cryptographic vulnerabilities affect IoMT devices, telemedicine platforms, cloud-based EHRs, and clinical decision-support systems [23].

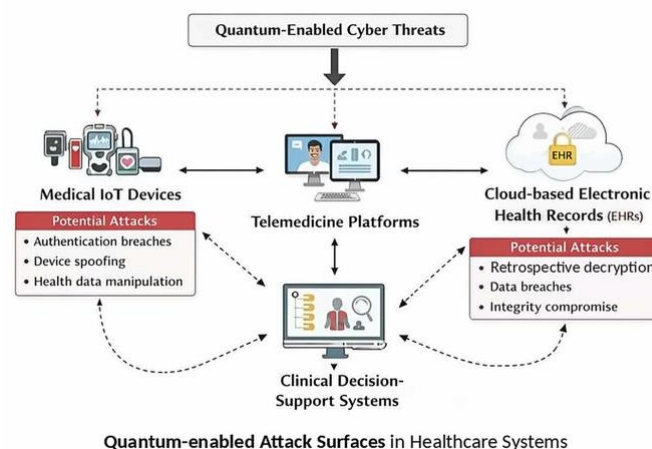


Figure 3: Quantum-enabled attack surfaces across interconnected healthcare systems

Hybrid quantum-classical cryptographic deployments represent a practical transitional approach for healthcare systems. These deployments combine classical cryptographic algorithms with post-quantum primitives, enabling backward compatibility while gradually reducing exposure to quantum risks. Hybrid key exchange and signature schemes are particularly relevant for healthcare infrastructures that involve long software life cycles and legacy medical devices. By leveraging both classical and quantum-resistant mechanisms, hybrid deployments mitigate the risk of premature migration failures while providing resilience against future quantum adversaries. Quantum Key Distribution (QKD) is a completely different paradigm of security because it takes advantage of quantum mechanics physical characteristics to create secure cryptography keys. In contrast to traditional protocols of key exchange, QKD allows identifying an eavesdropping attack by measuring observable perturbations to quantum states. QKD is particularly useful in healthcare settings in order to achieve high-sensitivity communication, including inter-hospital data exchange, partnerships with medical research institutions, and critical care networks. Nevertheless, QKD introduction is still limited by infrastructure needs, geographical distance, and the complexity of its integration, and it can be used in backbone healthcare networks but not resource-constrained edge devices. Quantum Random Number Generation (QRNG) enhances cryptographic robustness by producing true randomness derived from quantum phenomena. High-quality randomness is a foundational requirement for secure encryption, authentication, and key generation. In healthcare systems, QRNG can strengthen both classical and post-quantum cryptographic protocols by eliminating predictability in cryptographic keys and session parameters. Compared to QKD, QRNG is easier to integrate into existing infrastructures and can be deployed in both centralized healthcare data centers and distributed medical devices, providing immediate security benefits without extensive architectural changes [8].

Table 1: Quantum-Enabled Cybersecurity Threats Across Healthcare Technologies

Healthcare System	Primary Quantum-Enabled Threats	Potential Impact	Risk Level
Medical IoT Devices	Compromised authentication, key extraction, device spoofing	Patient safety risks, data manipulation, unauthorized device control	High
Telemedicine Platforms	Encrypted session interception, impersonation attacks	Privacy breaches, loss of patient trust, regulatory violations	High
Cloud-based EHR Systems	Retrospective decryption, data integrity attacks	Large-scale data breaches, compliance failures	Very High
Clinical Decision-Support Systems	Model manipulation, data poisoning	Incorrect diagnoses, unsafe treatment decisions	High
Wearables and Remote Monitoring	Data interception and falsification	Misleading health analytics, delayed interventions	Medium

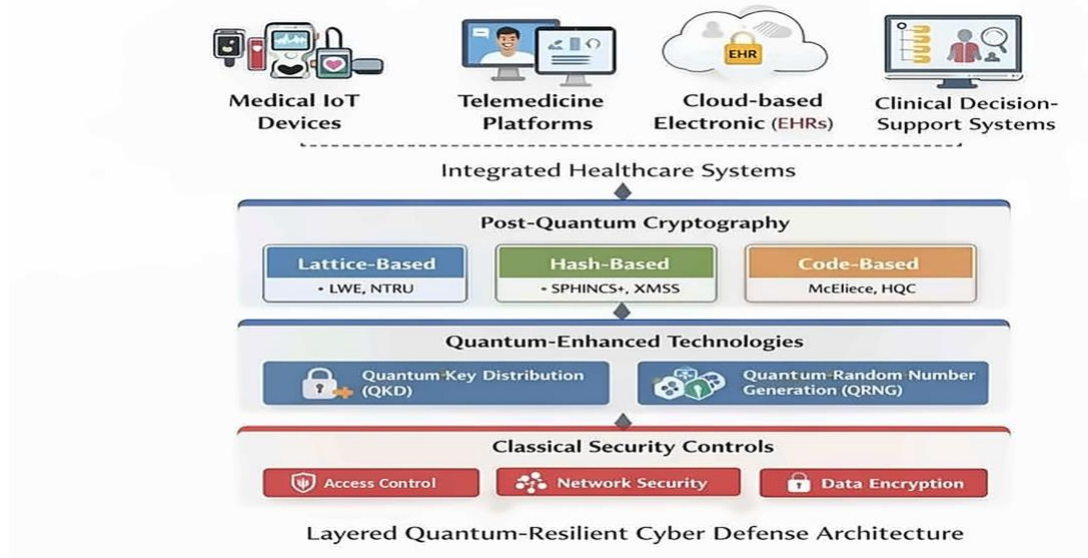


Figure 4: Quantum-resilient cyber defense architecture

Figure 4 conceptually illustrates a layered quantum-resilient cyber defense architecture for healthcare systems. The architecture integrates post-quantum cryptographic primitives, quantum-enhanced technologies, and classical security controls to form a defense-in-depth model. This layered approach ensures that the compromise of a single security mechanism does not cascade into systemic failure, thereby enhancing overall resilience. Effective quantum-resilient defense strategies must also account for operational constraints within healthcare environments. Medical systems often prioritize availability and real-time responsiveness, limiting the feasibility of computationally intensive security mechanisms. Consequently, defense solutions must be carefully selected based on system criticality, data sensitivity, and resource availability. For example, while QKD may be appropriate for securing inter-organizational data exchange, post-quantum cryptographic algorithms and QRNG may be more suitable for edge devices and wearable technologies [24].

Table 2 summarizes key quantum-enhanced and hybrid defense mechanisms and maps them to their primary security functions and healthcare applicability. This comparison highlights that no single defense mechanism addresses all security requirements, reinforcing the need for integrated and adaptive security architectures. Despite their promise, quantum-enhanced defense mechanisms introduce new challenges related to deployment cost, interoperability, and standardization. Healthcare organizations must balance security improvements against operational feasibility and regulatory requirements. Furthermore, the absence of mature deployment frameworks for some quantum technologies necessitates cautious adoption and rigorous evaluation [25, 26].

6. Regulatory, ethical, and governance considerations

The transition toward quantum-secure healthcare systems extends beyond technical implementation and raises significant regulatory, ethical, and governance challenges. Healthcare environments operate under strict legal and compliance frameworks designed to protect patient privacy, ensure data integrity, and maintain system availability. As quantum computing threatens the cryptographic foundations of existing security infrastructures, regulators, policymakers, and healthcare organizations must proactively adapt governance models to address emerging quantum-era risks [1].

From a regulatory perspective, the confidentiality, integrity, and availability of sensitive medical data are required by the laws of data protection in healthcare, particularly: the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and the laws of individual regions. The security requirements these regulations impose are mostly technology-independent, but its implicit security expectations have been to rely on the soundness of modern cryptographic protocols. This assumption is being challenged by the development of quantum computing since encryption schemes that are considered to be secure today can become compromised before the end of the retention period of the healthcare data. This is why forward-looking security strategies that include post-quantum cryptography standards and long-term risk evaluation are becoming more important to the regulatory compliance of the quantum era. Compliance-wise, such frameworks as HIPAA and GDPR implicitly demand that healthcare organizations implement security measures that guarantee long-term confidentiality and integrity of sensitive medical data. When it comes to emerging quantum threats, this requirement goes beyond existing cryptographic sufficiency to encompass readiness to counter future risks of decryption [2]. An example of this is that the existence of harvest-now, decrypt-later attacks is a direct challenge to the assumption of the security of encrypted data over the long term required by healthcare standards. This results in early migration to post-quantum cryptographic solutions, not only a technical improvement but also a regulatory imperative. By implementing quantum-resistant security control mechanisms proactively, healthcare institutions can be in a position to comply with regulatory standards by reducing the risks exposed over time, maintaining patient confidentiality, and ensuring sustained trust in digital healthcare systems [18].

Table 2: Quantum-enhanced and hybrid cyber defense mechanisms for healthcare

Defense Mechanism	Primary Security Function	Healthcare Applicability
Hybrid PQC-Classical Cryptography	Transitional quantum resistance, backward compatibility	Legacy systems, medical devices, EHR platforms
Quantum Key Distribution (QKD)	Secure key exchange with eavesdropping detection	Hospital networks, inter-institutional communication
Quantum Random Number Generation (QRNG)	High-entropy key and parameter generation	Data centers, medical devices, authentication systems
Blockchain with PQC Signatures	Data integrity, auditability, trust management	Medical records, consent tracking, data provenance

One of the most pressing regulatory challenges lies in defining acceptable timelines for cryptographic migration. Healthcare organizations often maintain patient records for decades, particularly in cases involving chronic illness, genetic data, or longitudinal studies. Regulatory bodies may therefore need to revise compliance guidelines to explicitly address quantum resilience, encouraging or mandating the adoption of post-quantum cryptography for systems handling long-lived medical data. Standardization initiatives led by institutions such as the National Institute of Standards and Technology (NIST) play a critical role in shaping these regulatory transitions by providing vetted cryptographic algorithms suitable for widespread deployment [16, 17, 27].

Ethical considerations further complicate the adoption of quantum-secure technologies in healthcare. Patient trust is a foundational element of medical practice, and any perceived weakness in data protection can undermine confidence in digital health systems. The ethical principle of patient autonomy requires that individuals have assurance regarding how their health data is stored, processed, and protected over time. Failure to anticipate quantum-enabled threats may result in retrospective data breaches that violate patient

consent and expose sensitive medical histories long after data collection. Equity and access also represent ethical dimensions of quantum-secure healthcare. Advanced cryptographic and quantum-enhanced technologies may impose significant financial and technical burdens, potentially widening disparities between well-resourced healthcare institutions and smaller providers. Ethical governance frameworks must therefore balance the imperative for robust security with considerations of accessibility and fairness, ensuring that quantum-secure solutions do not inadvertently exclude under-resourced healthcare systems or populations [28]. Governance challenges arise from the complexity and interconnectedness of modern healthcare ecosystems. Healthcare data is rarely confined to a single organization; instead, it flows across hospitals, laboratories, insurers, research institutions, and cloud service providers. Effective quantum-secure governance requires coordinated policies that align security practices across organizational boundaries. This includes establishing shared responsibility models for cryptographic updates, incident response, and risk management in the face of quantum-enabled threats [29, 30].

Long software life cycles and legacy medical devices further complicate governance efforts. Many certified medical devices cannot be easily updated without extensive revalidation, creating governance dilemmas regarding acceptable residual risk. Policymakers and healthcare administrators must therefore develop adaptive governance frameworks that support phased migration strategies, hybrid cryptographic deployments, and continuous risk evaluation. Such frameworks should prioritize patient safety while enabling incremental adoption of quantum-resilient technologies. Transparency and accountability are essential components of quantum-secure governance. Healthcare organizations must be able to demonstrate compliance with evolving security requirements and provide clear audit trails for cryptographic decisions. Technologies such as blockchain-based audit logs and cryptographically verifiable access controls can support accountability while reinforcing trust among stakeholders [12, 28]. However, governance frameworks must carefully evaluate the long-term security of these technologies in a quantum context to avoid introducing new vulnerabilities. International collaboration represents another critical governance dimension. Healthcare data frequently crosses national borders for research, treatment, and public health monitoring. Divergent regulatory approaches to quantum security could create interoperability challenges and compliance conflicts. Harmonization of post-quantum cryptographic standards and regulatory expectations at the international level will therefore be essential to support secure global healthcare collaboration in the quantum era. Regulatory, ethical, and governance considerations are central to the successful adoption of quantum-secure healthcare systems. Technical solutions alone are insufficient without supportive legal frameworks, ethical safeguards, and coordinated governance structures. Proactive regulatory adaptation, ethically grounded security practices, and collaborative governance models will be necessary to ensure that quantum-resilient technologies enhance patient trust, protect sensitive medical data, and support sustainable digital healthcare ecosystems [5, 19].

7. Conclusion and future research directions

The rapid advancement of quantum computing poses a fundamental challenge to the security foundations of modern healthcare systems. As this review has demonstrated, the cryptographic mechanisms currently protecting electronic health records, medical IoT devices, telemedicine platforms, and clinical decision-support systems are increasingly vulnerable to quantum-enabled attacks. Given the long-term sensitivity of healthcare data and the critical role of digital technologies in patient care, proactive transition toward quantum-resilient security architectures is no longer optional but essential. This paper presented a comprehensive analysis of the quantum threat landscape in healthcare and systematically examined post-quantum cryptographic solutions and quantum-enhanced defense mechanisms. By synthesizing existing

research on post-quantum cryptography, hybrid quantum-classical security models, quantum key distribution, quantum random number generation, and blockchain-based trust systems, the study highlighted the strengths and limitations of current approaches in real-world healthcare environments. The analysis further demonstrated that no single technology can address all security requirements, underscoring the necessity of layered, defense-in-depth strategies tailored to heterogeneous healthcare infrastructures. Beyond technical considerations, this review emphasized the importance of regulatory compliance, ethical responsibility, and governance frameworks in enabling the adoption of quantum-secure healthcare systems. Ensuring patient privacy, maintaining trust, and achieving interoperability across institutions require coordinated efforts among policymakers, healthcare providers, technology vendors, and standardization bodies. Early alignment with emerging post-quantum standards is critical to mitigating long-term risks associated with retrospective decryption and systemic cryptographic failure.

Future research should focus on several key directions. First, empirical evaluation of post-quantum cryptographic algorithms in resource-constrained medical devices and real-time healthcare applications is needed to assess performance and scalability trade-offs. Second, the development of adaptive hybrid security frameworks that support gradual migration while maintaining backward compatibility remains an open challenge. Third, integration of quantum-resilient security with AI-driven clinical systems warrants further investigation to safeguard data integrity and decision reliability. Finally, interdisciplinary research combining cryptography, healthcare informatics, policy, and ethics will be essential to design governance models that are both secure and socially responsible. Achieving quantum-secure healthcare requires early action, strategic planning, and collaborative innovation. By adopting post-quantum cryptographic standards and layered cyber defense approaches, healthcare systems could protect sensitive medical data, ensure regulatory compliance, and sustain trust in next-generation digital health ecosystems in the approaching quantum era.

Funding Statement: The author received no specific funding for this study.

Data Availability: No new data used in this research.

Conflicts of Interest: The authors declare no conflicts of interest.

Authors contributions. Conceptualization: ARB, MA ; data curation and methodology: ARB, MA, MAR, SS; validation and visualization: MAR, SS; writing original draft: ARB, MA, MAR, SS ; writing review and editing: ARB, MA; supervision and project administration: ARB, MA. The authors had approved the final version.

AI Usage Disclosure

Artificial intelligence tool Grammarly was used only for language polishing and grammatical correction. All scientific and technical contents were created and validated by the authors.

Ethical approval: Not applicable

References

- [1] 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.
- [2] Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., et al., (2025). "Advancing security in cloud-based patient information systems with quantum-resistant encryption for healthcare data". *Asian Journal of Research in Computer Science*, 18(4), 187-208.
- [3] Fathalla, E., and Azab, M. (2024). "Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations". *IEEE Access*, 12, 175969-175987.
- [4] Fitzgibbon, G., and Ottaviani, C. (2024). "Constrained device performance benchmarking with the implementation of post-quantum cryptography". *Cryptography*, 8(2), 21.
- [5] Saberi Kamarposhti, M., Ng, K. W., Chua, F. F., et al., (2024). "Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data". *Heliyon*, 10(10), e31406.
- [6] Ahmad, A., and Jagatheswari, S. (2024). "Lattice-based three party authenticated key agreement scheme in medical IoT for post-quantum environment". *IEEE Access*, 12, 157247-157259.
- [7] Näther, C., Herzinger, D., Gazdag, S.-L., et al., (2024). "Migrating software systems toward post-quantum cryptography—A systematic literature review". *IEEE Access*, 12, 132107-132126.
- [8] Sahu, S. K., and Mazumdar, K. (2024). "State-of-the-art analysis of quantum cryptography: Applications and future prospects". *Frontiers in Physics*, 12, 1456491.
- [9] Mehmood, A., Shafique, A., Alawida, M., et al., (2024). "Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques". *IEEE Access*, 12, 27530-27555.
- [10] Liu, Y. K., and Moody, D. (2024). "Post-quantum cryptography and the quantum future of cybersecurity". *Physical Review Applied*, 21(4), 040501.
- [11] Gharavi, H., Granjal, J., and Monteiro, E. (2024). "Post-quantum blockchain security for the Internet of Things: Survey and research directions". *IEEE Communications Surveys & Tutorials*, 26(3), 1748-1774.
- [12] Sezer, B. B., Akleylek, S., and Nuriyev, U. (2025). "PP-PQB: Privacy-preserving in post-quantum blockchain-based systems: A systematization of knowledge". *IEEE Access*, 13, 41382-41405.
- [13] Singh, N., Singh, S. K., Kumar, S., et al., (2024). "Next gen security with quantum-safe cryptography". In *Advances in Information Security, Privacy, and Ethics*, IGI Global, 133-166.
- [14] Boujelben, M., and Abid, M. (2024). "Post-quantum security design for hierarchical healthcare systems based on lattices". *The Journal of Supercomputing*, 80(12), 17292-17313.
- [15] Fernández-Caramés, T. M. (2020). "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things". *IEEE Internet of Things Journal*, 7(7), 6457-6480.
- [16] National Institute of Standards and Technology (2024). "Module-lattice-based key-encapsulation mechanism standard". *Federal Information Processing Standards Publication (FIPS) 203*, NIST, Gaithersburg, MD.
- [17] National Institute of Standards and Technology (2024). "Module-lattice-based digital signature standard". *Federal Information Processing Standards Publication (FIPS) 204*, NIST, Gaithersburg, MD.
- [18] Rubio García, C., Rommel, S., Takarabt, S., et al., (2024). "Quantum-resistant transport layer security". *Computer Communications*, 213, 345-358.
- [19] Sabrina, F., Sohail, S., and Tariq, U. U. (2024). "A review of post-quantum privacy preservation for IoMT using blockchain". *Electronics*, 13(15), 2962.
- [20] Alsadhan, A., Alhogail, A., and Alsalamah, H. (2024). "Blockchain-based privacy preservation for the Internet of Medical Things: A literature review". *Electronics*, 13(19), 3832.
- [21] Tahir, N. U. A., Rashid, U., Hadi, H. J., et al., (2024). "Blockchain-based healthcare records management framework: Enhancing security, privacy, and interoperability". *Technologies*, 12(9), 168.

- [22] Fonsêca, A. L. A., Barbalho, I. M. P., Fernandes, F., et al., (2024). "Blockchain in health information systems: A systematic review". *International Journal of Environmental Research and Public Health*, 21(11), 1512.
- [23] Sharma, N., and Dhiman, P. (2025). "A survey on IoT security: Challenges and their solutions using machine learning and blockchain technology". *Cluster Computing*, 28, 313.
- [24] Lakhan, A., Mohammed, M. A., Nedoma, J., et al., (2023). "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare". *IEEE Journal of Biomedical and Health Informatics*, 27(2), 664-672.
- [25] Alsaeed, N., Nadeem, F., and Albalwy, F. (2024). "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing". *Future Generation Computer Systems*, 151, 162-181.
- [26] Prajapat, S., Kumar, P., Kumar, D., et al., (2024). "Quantum secure authentication scheme for Internet of Medical Things using blockchain". *IEEE Internet of Things Journal*, 11(23), 38496-38507.
- [27] National Institute of Standards and Technology (2024). "Stateless hash-based digital signature standard". *Federal Information Processing Standards Publication (FIPS) 205*, NIST, Gaithersburg, MD.
- [28] Wani, R. U. Z., Thabit, F., and Can, O. (2024). "Security and privacy challenges, issues, and enhancing techniques for Internet of Medical Things: A systematic review". *Security and Privacy*, 7(5), e409.
- [29] Adil, M., Khan, M. K., Jadoon, M. M., et al., (2023). "An AI-enabled hybrid lightweight authentication scheme for intelligent IoMT based cyber-physical systems". *IEEE Transactions on Network Science and Engineering*, 10(5), 2719-2730.
- [30] Zachos, G., Essop, I., Mantas, G., et al., (2021). "An anomaly-based intrusion detection system for Internet of Medical Things networks". *Electronics*, 10(21), 2562.