Strengthening Healthcare Data Security Using Quantum-Resistant Cryptography

Shiv Shankar Dwivedi[1], Santosh Kumar Sharma[2]

[1]Department of Computer Science & Engineering, United University Prayagraj, India
*Corresponding Author Email: ssdwivedikec@gmail.com

[2]Department of Computer Science & Engineering, United University Prayagraj, India
Email: sharma.santosh83@gmail.com

Abstract

The digitization of the healthcare sector has revolutionized the way patients receive care, how medicine is researched, and the way health information is managed. EHRs, telemedicine systems, health wearables, cloud computing, and artificial intelligence have made healthcare delivery much more efficient than ever before. On the other hand, the growing reliance on digital infrastructure in healthcare organizations leaves such companies vulnerable to complex cyber-attacks. The current cryptographic mechanisms that protect health-related information in healthcare organizations like RSA and ECC can be compromised by large-scale quantum computing. Quantum computing can use quantum algorithms like Shor's algorithm to break down the current popular public key cryptography. For this reason, healthcare organizations need to adapt to new Quantum Resistant Cryptography (QRC) or Post-Quantum Cryptography (PQC). This chapter focuses on the significance of health data security, quantum computing challenge, approaches to quantum-resistant cryptography, methods for implementing QRC, regulatory concerns, challenges, and future directions.

Keywords: Healthcare cyber security, Post-Quantum Cryptography, Quantum-Resistant Cryptography, Electronic Health Records, Data Privacy, HIPAA, Healthcare Information Security.

How to cite this article: Dwivedi SS, Sharma SK. Strengthening Healthcare Data Security Using Quantum-Resistant Cryptography. Int J Drug Deliv Technol. 2026;16(63s):1685-1690. DOI: 10.25258/ijddt.16.63s.172

1. Introduction

Health care data represents one of the most valuable categories of personal information. Medical-records contain demographic information, diagnostic-reports, treatment histories, genomic profiles, insurance details, and financial information. The cumulative acceptance of Electronic-Health-Records (EHRs) has enhanced healthcare efficiency but has simultaneously expanded the attack surface for cybercriminals.

Healthcare organizations worldwide experience frequent ransomware attacks, data breaches, and unauthorized access incidents. The healthcare sector remains an attractive target because patient data commands high value in illegal markets and because disruption of healthcare services can directly impact human lives.

The existing approach for ensuring cyber security is based largely on the use of public key cryptographic schemes like RSA and ECC. Though these schemes are very secure today, future advancements in quantum computing can jeopardize their security. Therefore, it would be wise to adopt quantum-safe encryption techniques.

2. Healthcare Data Security: Current Landscape

Healthcare organizations generate and manage enormous quantities of sensitive information. These include:

2.1 Types of Healthcare Data

- Electronic-Health-Records (EHRs)
- Personal-Health-Information (PHI)
- Medical imaging records
- Laboratory reports
- Genomic and proteomic data
- Insurance information
- Clinical trial data
- Telemedicine communications

2.2 Major Security Threats

2.2.1 Ransomware Attacks

Healthcare institutions frequently face ransomware attacks that encrypt critical medical data and disrupt healthcare operations.

2.2.2 Data Breaches

Unauthorized access to patient records may result in identity theft, financial fraud, and privacy violations.

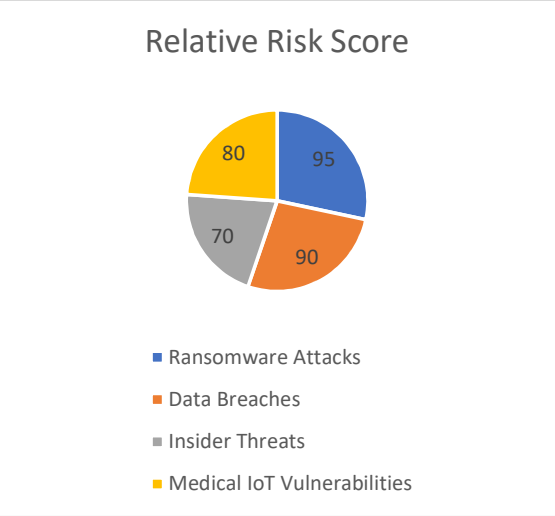

Figure 1. Relative impact of major cyber security threats affecting healthcare organizations.

2.2.3 Insider Threats

Healthcare-employees may deliberately or inadvertently compromise sensitive information.

2.2.4 Medical IoT Vulnerabilities

Connected medical devices such as infusion pumps, cardiac monitors, and wearable sensors introduce additional security risks.

2.3 Security Requirements in Healthcare

Healthcare cyber security frameworks focus on:

- Confidentiality
- Integrity
- Availability
- Authentication
- Non-repudiation
- Accountability

These principles form the foundation of healthcare information protection.

3. Understanding Quantum Computing

Quantum computing represents a revolutionary computational paradigm based on quantum mechanics.

3.1 Qubits and Quantum States

Contrary to classical bits, which have two possible values, a quantum bit (qubit) can assume more than one value simultaneously due to the phenomenon of superposition.

3.2 Quantum Entanglement

Quantum entanglement enables the performance of qubits' correlated operations necessary for parallel computation.

3.3 Quantum Algorithms

The following two quantum algorithms will be helpful in understanding cryptography-related applications:

Shor's Algorithm

Can factorize large numbers and defeat RSA, DH, and ECC.

Grover's Algorithm

Improves brute-force attack speeds on symmetric cryptosystems.

4. The Quantum Threat to Healthcare Security

4.1 Vulnerability of Current Cryptographic Systems

Healthcare organizations currently use:

- RSA
- ECC
- Diffie-Hellman Key Exchange
- Digital Signature Algorithms

Large-scale quantum computers could compromise these systems.

4.2 Harvest-Now Decrypt- Later Attacks

Cyber criminals may collect encrypted healthcare-data today and decrypt it in the future once quantum computing becomes practical.

This threat is especially significant for:

- Lifetime patient records
- Genomic information
- Clinical trial data
- National health databases

4.3 Long-Term Data Protection Requirements

Healthcare information often requires protection for decades. Consequently, organizations must prepare for quantum threats before quantum computers become operational at scale.

Table 1. Comparison between conventional cryptographic systems and quantum-resistant cryptographic approaches in healthcare.

Feature	Classical Cryptography (RSA/ECC)	Quantum-Resistant Cryptography (PQC)
Security against classical attacks	High	High
Security against quantum attacks	Vulnerable	Resistant
Key exchange	RSA, Diffie-Hellman	CRYSTALS-Kyber
Digital signatures	RSA, ECDSA	Dilithium, Falcon, SPHINCS+
Long-term protection	Limited	Strong
Healthcare suitability	Current standard	Future-ready
NIST recommendation	Being phased out	Recommended

5. Quantum-Resistant Cryptography

Quantum-Resistant Cryptography (QRC) consists of cryptographic algorithms designed to remain secure against both classical and quantum attacks.

5.1 Objectives

- Secure data confidentiality
- Preserve digital signatures
- Enable secure communication
- Ensure long-term data protection

5.2 Post-Quantum Cryptography Categories

5.2.1 Lattice-Based Cryptography

Examples:

- CRYSTALS-Kyber
- CRYSTALS-Dilithium

Advantages:

- Strong security
- Efficient implementation
- Suitable for healthcare networks

5.2.2 Code-Based Cryptography

Examples:

- Classic McEliece

Advantages:

- Long history of security
- Resistance to known quantum attacks

5.2.3 Hash-Based Signatures

Examples:

- XMSS
- SPHINCS+

Advantages:

- Well-understood security properties

5.2.4 Multivariate Cryptography

Uses systems of multivariate polynomial equations.

5.2.5 Isogeny-Based Cryptography

Provides compact key sizes but remains under active research.

6. NIST Post-Quantum Cryptography Standardization

The National Institute of Standards and Technology (NIST) launched a global initiative to identify and standardize quantum-resistant algorithms.

Selected Algorithms

Key Encapsulation Mechanism

- CRYSTALS-Kyber

Digital Signatures

- CRYSTALS-Dilithium
- Falcon
- SPHINCS+

These standards provide a foundation for future healthcare cybersecurity systems.

7. Applications of Quantum-Resistant Cryptography in Healthcare

7.1 Electronic Health Records (EHRs)

Post-quantum encryption can protect patient records stored in hospital information systems and cloud environments.

7.2 Telemedicine Security

Secure communication between physicians and patients can be maintained through quantum-resistant key exchange mechanisms.

7.3 Medical Internet of Things (IoMT)

Connected healthcare devices can implement lightweight post-quantum protocols to resist future cyber threats.

7.4 Genomic Data Protection

Genomic information remains sensitive throughout an individual's lifetime, making quantum-resistant encryption particularly important.

7.5 Cloud-Based Healthcare Systems

Healthcare cloud platforms can integrate post-quantum cryptographic protocols for secure data storage and transmission.

Table 2. Major healthcare applications benefiting from quantum-resistant cryptography.

Healthcare Domain	Sensitive Data Protected	PQC Benefit
Electronic Health Records (EHRs)	Patient medical records	Long-term confidentiality
Telemedicine	Audio/video consultations	Secure communication
Medical IoT Devices	Sensor-generated data	Protection against future attacks
Genomic Databases	DNA and genetic information	Lifetime privacy protection
Cloud Healthcare Systems	Stored patient records	Secure cloud storage
Clinical Trials	Research and participant data	Data integrity and confidentiality

8. Healthcare Regulatory Compliance and Quantum Security

8.1 HIPAA

HIPAA mandates ePHI security as part of its guidelines.

Quantum resistant cryptography will ensure compliance through increased protection mechanisms.

8.2 GDPR

The General Data Protection Regulation focuses on strong security controls and privacy by design.

8.3 HITECH Act

Promotes secure adoption of healthcare information technology.

8.4 National Digital Health Policies

Countries implementing digital health missions should incorporate post-quantum security strategies into future healthcare infrastructure.

9. Implementation Framework for Healthcare Organizations

Phase 1: Cryptographic Inventory

Organizations should identify all cryptographic assets and dependencies.

Phase 2: Risk Assessment

Evaluate systems vulnerable to quantum attacks.

Phase 3: Pilot Deployment

Implement hybrid cryptographic architectures combining traditional and post-quantum algorithms.

Phase 4: Migration Strategy

Gradually replace vulnerable systems with standardized quantum-resistant solutions.

Phase 5: Continuous Monitoring

Regular security assessments ensure ongoing protection.

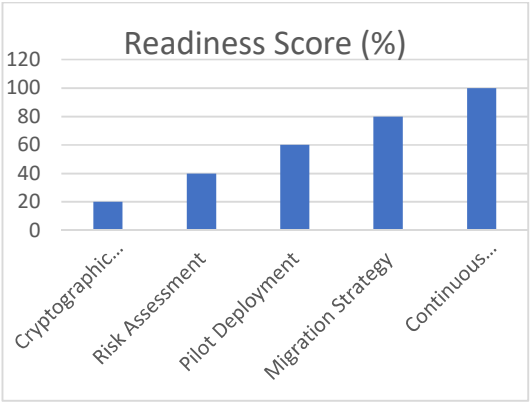

Figure 2. Progressive implementation roadmap for quantum-resistant cryptography adoption in healthcare organizations.

10. Challenges in Adopting Quantum-Resistant Cryptography

10.1 Computational Overhead

Some post-quantum algorithms require larger keys and signatures.

10.2 Legacy Infrastructure

Healthcare institutions often rely on older systems that may not support modern cryptographic standards.

10.3 Cost Considerations

Migration requires investment in software updates, hardware upgrades, and workforce training.

10.4 Interoperability Issues

Healthcare systems must maintain compatibility across diverse platforms.

10.5 Regulatory Uncertainty

Global regulatory frameworks are still evolving regarding post-quantum cybersecurity requirements.

11. Best Practices for Healthcare Organizations

- Develop a post-quantum cybersecurity roadmap.
- Conduct cryptographic audits regularly.
- Implement hybrid encryption strategies.
- Adopt NIST-approved algorithms.
- Train healthcare IT personnel.
- Secure medical IoT ecosystems.
- Strengthen cloud security controls.
- Establish incident response mechanisms.
- Continuously monitor emerging quantum threats.

12. Future Perspectives

The transition toward quantum-safe healthcare systems will accelerate over the coming decade. Emerging technologies such as blockchain-based healthcare records, artificial intelligence, and precision medicine will require robust cryptographic foundations. International collaboration among healthcare providers, cyber security experts, standards organizations, and policymakers will be essential to achieve secure and resilient healthcare infrastructures.

Quantum-resistant cryptography is expected to become a critical component of healthcare cyber security frameworks worldwide. Early adoption can reduce future risks and protect sensitive patient information against both current and future cyber threats.

13. Conclusion

The use of technology to provide healthcare services is becoming widespread in today's healthcare environment. While these technologies offer many advantages in providing better healthcare services, diagnostics, and research, they raise several cybersecurity concerns. The introduction of quantum computing poses an imminent danger to classical cryptosystems that have thus far protected medical data. Quantum-resistant cryptography presents itself as a promising approach to securing patient information against quantum attacks. Through using quantum cryptography protocols, performing cybersecurity risk assessments, and adhering to healthcare regulations, the security of healthcare data can be assured.

References

1. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. Proc 35th Annual Symposium on Foundations of Computer Science. 1994;124–134.
2. Grover LK. A fast quantum mechanical algorithm for database search. Proc 28th Annual ACM Symposium on Theory of Computing. 1996;212–219.
3. National Institute of Standards and Technology. Post-Quantum Cryptography Standardization Project. Gaithersburg: NIST; 2024.
4. Barker E, Roginsky A. Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST Special Publication 800-131A Rev.2. 2019.
5. Alagic G, et al. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8413. 2022.
6. Chen L, Jordan S, Liu YK, Moody D, Peralta R, Perlner R, et al. Report on Post-Quantum Cryptography. NIST IR 8105. 2016.
7. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson; 2023.
8. Koblitz N, Menezes A. The random oracle model: a twenty-year retrospective. Des Codes Cryptogr. 2015;77(2-3):587-610.

9. Bernstein DJ, Buchmann J, Dahmen E. Post-Quantum Cryptography. Berlin: Springer; 2009.

10. Hülsing A, Butin D, Gazdag S, Rijneveld J, Mohaisen A. XMSS: Extended Merkle Signature Scheme. RFC 8391. 2018.

11. Bernstein DJ, Lange T. Post-quantum cryptography. Nature. 2017;549(7671):188-194.

12. Ponemon Institute. Cost of a Data Breach Report. IBM Security; 2024.

13. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review. Technol Health Care. 2017;25(1):1-10.

14. McLeod A, Dolezel D. Cyber-analytics: modeling factors associated with healthcare data breaches. Decis Support Syst. 2018;108:57-68.

15. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic review. J Med Internet Res. 2018;20(5):e10059.

16. Office for Civil Rights. Health Insurance Portability and Accountability Act (HIPAA) Security Rule Guidance. Washington DC; 2024.

17. European Union. General Data Protection Regulation (GDPR). Official Journal of the European Union. 2018.

18. National Academies of Sciences. Quantum Computing: Progress and Prospects. Washington DC: National Academies Press; 2019.

19. Aggarwal D, Brennen GK, Lee TK, Santha M, Tomamichel M. Quantum attacks on Bitcoin and blockchain. Ledger. 2018;3:68-90.

20. Mosca M. Cybersecurity in an era with quantum computers: will we be ready? IEEE Security Privacy. 2018;16(5):38-41.

21. Healthcare Information and Management Systems Society (HIMSS). Healthcare Cybersecurity Survey Report. Chicago: HIMSS; 2024.

22. World Health Organization. Global Strategy on Digital Health 2020–2025. Geneva: WHO; 2021.