Quantum-Resistant Cryptography Migration Strategies for Long-Term Data Security in Healthcare

Author: Amelia Roberts **Affiliation:** Department of Computer Science, University of Manchester (UK)

Email: amelia.roberts@manchester.ac.uk

Abstract

Healthcare systems store and process sensitive patient data with long retention requirements. The advent of quantum computing poses a future threat to public-key cryptographic primitives widely used for confidentiality, integrity, and authentication. This paper presents a comprehensive, practically actionable framework for migrating healthcare information systems to quantum-resistant cryptography (post-quantum cryptography, PQC). We combine a technical primer on PQC (algorithm families, security proofs, parameter choices), formal definitions (IND-CPA/CCA, EUF-CMA), and mathematical formulations (Learning With Errors, Ring-LWE, code-based hardness) with a detailed migration lifecycle: inventory and risk assessment, prioritized upgrade paths, hybrid deployments, cryptographic agility, key management, archival re-protection, performance evaluation, compliance mapping (HIPAA, local law), and a multi-year roadmap. We include analysis of interoperability challenges in TLS and cloud services, propose benchmarks and testing methodology, and supply recommended policies and timelines tailored to healthcare's long data-retention periods. The strategy is grounded in current standards work (NIST PQC), national guidance (NCCoE, NCSC), recent literature, and implementation case studies.

Key recommendations: adopt hybrid key-establishment for internet-facing services immediately; implement cryptographic-agility abstraction layers in middleware; prioritize protection of archived and “harvest-now-decrypt-later” high-value datasets; perform pilot deployments for selected PQC KEMs and signature schemes; and prepare re-encryption plans for long-term archives.

Keywords: Post-quantum cryptography, migration strategy, healthcare data, cryptographic agility, lattice-based cryptography, hybrid cryptography, long-term data security, HIPAA, NIST PQC.

1. Introduction

The integrity, confidentiality, and authenticity of electronic health records (EHRs), imaging, genomic datasets, and clinical analytics underpin modern healthcare. These datasets are often retained for decades, creating an acute need to plan for “cryptanalytic harvest now, decrypt later” attacks: adversaries may capture encrypted archives today and decrypt them after sufficiently powerful quantum computers become available. The timeline for a cryptanalytically-relevant quantum computer (CRQC) is uncertain; however, risk management requires forward planning and migration readiness. National bodies and industry leaders have accelerated PQC standardization and migration guidance (e.g., NIST PQC announcements and NCCoE migration projects), recognizing the urgency for sectors with long-lived secrets such as healthcare.

This paper responds to the need for a domain-specific migration strategy for healthcare organizations. We combine cryptographic theory, standard guidance, and practical engineering to produce an actionable migration plan that balances security, interoperability, performance, and regulatory compliance.

2. Background and Related Work

2.1 Quantum threats to classical public-key cryptography

Quantum algorithms primarily Shor's algorithm can efficiently solve integer factorization and discrete logarithm problems, rendering RSA and ECC insecure against future quantum adversaries. Symmetric primitives and hash functions are more resilient: Grover's algorithm yields quadratic speedups but can be mitigated by doubling key sizes. Post-quantum cryptography aims to replace quantum-vulnerable public-key primitives with algorithms believed secure against both classical and quantum adversaries (e.g., lattice-based, code-based, hash-based, multivariate). NIST's multi-year selection process has formalized candidate algorithms and released finalized standards.

2.2 Healthcare-specific concerns and publication landscape

Healthcare's long retention, strict privacy rules (HIPAA in the U.S.), and complex cloud/hybrid infrastructures magnify migration challenges. Recent literature frames the healthcare PQC problem and offers roadmaps and sectoral guidance. SaberiKamarposhti et al. (2024) surveyed the healthcare implications and produced a focused roadmap for PQC adoption in medical systems. National cyber guidance (NCSC and NCCoE) target phased migration approaches. Industry whitepapers (e.g., Mastercard) and practical hybrid TLS research provide blueprints for gradual transitions.

2.3 Prior research on PQC migration

Analyses of hybrid approaches, performance tradeoffs, and algorithm-specific implementation concerns have been published in the last 3–5 years (papers on lattice-based performance, code-based integrations, SPHINCS+, and performance frameworks for PQ-TLS). These works inform our recommendations for pilot choices and benchmarks.

3. Cryptographic Primer Algorithms, Security Models and Hardness Assumptions

This section defines formal security notions and describes the principal families of PQC algorithms.

3.1 Security definitions

IND-CPA and IND-CCA (KEMs & PKE):

- A public-key encryption (PKE) scheme is IND-CPA secure if no efficient adversary can distinguish encryptions of chosen messages given only public key access. Formally, for adversary A, advantage:

$$\text{Adv}^{\mathcal{A}}_{\text{IND-CPA}}(\lambda) =\mid \Pr[\mathcal{A}(pk, \mathcal{E}(pk, m_0)) = 1] - \Pr[\mathcal{A}(pk, \mathcal{E}(pk, m_1)) = 1] \mid$$

for messages m_0, m_1chosen by the adversary. For KEMs used in TLS, IND-CCA security is typically required.

EUF-CMA (Signatures):

- A digital signature scheme is existentially unforgeable under chosen message attack (EUF-CMA) if a polynomial-time adversary cannot produce a valid signature on any new message after querying signing oracles.

We require PQC candidates to maintain these properties against quantum adversaries (adversary modeled as quantum polynomial time). Security reductions commonly relate scheme breakability to underlying hard problems (e.g., LWE), with explicit bounds on advantage.

3.2 Lattice-based hardness: LWE and Ring-LWE

Learning With Errors (LWE): Given primes and parameters, given samples $(\mathbf{a}_i, b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i)$, where $\mathbf{s}$is secret and $e_i$from an error distribution, recover $\mathbf{s}$is hard. Formally, LWE problem with modulus q, dimension $n$and error distribution $\chi$is believed to be hard for both classical and quantum adversaries for appropriate parameters.

Ring-LWE: A structured variant providing efficiency via polynomial rings; underlying hardness reduces to ideal lattice problems and allows more compact keys and faster operations basis for many NIST candidate KEMs (e.g., CRYSTALS-KEM) and signature schemes.

Mathematical formulations of KEM correctness and security reductions are included in Appendix A (example reductions from IND-CPA of underlying PKE to hardness of LWE; parameter selection guidelines follow NIST recommendations).

3.3 Other families: code-based, hash-based, multivariate, isogeny-based

- **Code-based (McEliece variants):** Longstanding code-based schemes (McEliece) are resilient to quantum attacks but often have large public keys; certain new constructions attempt to reduce key sizes.
- **Hash-based (SPHINCS+):** Stateless designs for signatures, with strong security provenance tied to the collision resistance of underlying hashes. SPHINCS+ is NIST-approved as a post-quantum signature alternative.
- **Isogeny-based:** Smaller keys but recent concerns over security and performance exist; NIST selection trimmed candidate list.
- **Multivariate quadratic:** Fast signature verification and signing potential, but subject to structural attacks; fewer mature deployments.

4. Healthcare Threat Model & Requirements

4.1 Data types and retention

Healthcare data categories: EHRs, DICOM imaging, genomic sequences, clinical trial datasets, research data, backups, and logs. Retention policies vary: certain records must be kept for decades or indefinitely. This leads to a long exposure window for cryptanalytic harvest-and-decrypt strategies.

4.2 Adversary capabilities

- **Near-term:** State actors and large industry actors with significant classical compute and data collection capabilities.
- **Future quantum adversary (Q):** Capable of running Shor-style attacks on RSA/ECC once a CRQC is available. Planning for Q requires mitigations, not necessarily immediate complete rekeying, but preventing future decryption of captured ciphertexts.

4.3 Regulatory constraints and compliance

Healthcare organizations must maintain compliance with HIPAA Privacy and Security Rules (U.S.), GDPR for EU patients where applicable, and other national laws. These regulatory frameworks require appropriate safeguards for patient data, including risk assessment and technical controls; PQC migration must be aligned to avoid gaps in compliance. National guidance suggests migration planning now for long-lived data.

5. Migration Lifecycle & Strategy

We propose a pragmatic, phased migration lifecycle with justifications and action items tailored to healthcare.

5.1 Phase 0 Preparation and governance

- **Establish PQC governance working group:** stakeholders from IT, security, legal/compliance, clinical informatics, procurement.
- **Inventory cryptographic use cases:** endpoints, TLS, VPN, email, code signing, disk/encryption-at-rest, cloud KMS, archive formats. Prioritize assets by confidentiality value and retention period.

Actionables: cryptographic inventory tooling, data classification policy, risk register. Align schedule with institutional retention policies and the organization’s threat tolerance.

5.2 Phase 1 Immediate low-risk deployments and hybrid rollouts

- **Adopt hybrid KEMs for TLS endpoints:** combine classical and PQC KEMs in a hybrid key encapsulation within TLS handshake to preserve security under both classical and quantum assumptions (provides defense-in-depth). IETF drafts and implementer pilots advocate hybrid designs for safe transition.
- **Pilot PQ-ready code paths for device firmware, EHR client, and APIs** instrument crypto-agility layers (abstraction, feature flags, provider selection).

Rationale: hybrid modes mitigate immediate risk while providing operational telemetry for PQ algorithm performance.

5.3 Phase 2 Key management, archives, and re-encryption strategy

- **Protect archival data fast:** classify highest-value archives and either re-encrypt with PQC or apply envelope encryption with PQ-resistant key wrap. For extremely critical archives, perform post-compromise re-encryption (rekey) as an administrative and technical policy.
- **Design key rotation and backup plans:** consider rekey windows based on the assessed time to CRQC typical planning horizons in industry suggest 5–15 years depending on exposure. Implement hardware security modules (HSMs) with PQ-capability or firmware upgrade paths.

5.4 Phase 3 Full production migration & deprecation of vulnerable primitives

- **Deprecate standalone RSA/ECC for public-key operations** in favor of PQC or hybrid alternatives, after extensive testing and validation. Ensure signature algorithms used for long-term validation (e.g., code signing for medical device firmware) are PQ-resistant or employ layered signing strategies (dual signatures).
- **Vendor coordination:** require cloud providers and ISVs to offer PQC endpoints and contractual commitments for future migrations.

5.5 Phase 4 Continuous monitoring and review

- Continuous performance telemetry, interoperability testing, and security audits. Update plans as NIST finalizes additional standards and as new cryptanalytic knowledge emerges. National bodies encourage iterative review and readiness exercises.

6. Design Patterns and Engineering Controls

6.1 Cryptographic Agility

Implement an abstraction layer that decouples application logic from specific crypto algorithms. Design the layer to:

- Allow runtime selection of algorithms (classical, PQC, hybrid).
- Support key versioning and re-wrapping.
- Be testable in CI/CD; instrument to measure latency, key sizes, and error rates.

6.2 Hybrid mechanisms

Hybrid KEMs: if KEM1 provides classical security and KEM2 is PQC, derive session key as $K = \mathrm{KDF}(\mathrm{KEM1\_shared} \parallel \mathrm{KEM2\_shared})$. This reduces the risk that either primitive alone is broken. Hybrid signatures may be constructed by verifying both classical and PQ signatures or using compound signatures to ensure backward compatibility and long-term validity.

6.3 Key lifecycle & HSMs

- Use HSMs that are firmware-upgradeable for PQC algorithms or ensure vendor roadmap commitments.
- Archive keys under multi-party control and use threshold cryptography where possible to limit exfiltration risk.

6.4 Long-term archival and re-protection

For data retained > 10 years, we recommend either:

- **Re-encrypt on schedule**: periodic re-encryption with contemporary recommended algorithms (and store versioned ciphertexts); or
- **Use PQC envelope keys**: encrypt content keys with PQC KEMs (or hybrid wrappers) and store multiple wrappers to allow layered migration.

7. Interoperability & Performance Evaluation

7.1 TLS and Internet services

Deploy pilot PQ-TLS endpoints; measure handshake latency, CPU, and bandwidth overheads. Evaluate KEM choices: lattice-based KEMs often provide good performance; code-based may have larger keys; signature schemes vary drastically in size and latency (e.g., SPHINCS+ has larger signatures than ECDSA but is hash-based).

Performance frameworks for PQ-TLS and hybrid designs guide testing methodology. We recommend benchmarking both server and resource-constrained clients (medical devices, imaging scanners).

7.2 Cloud and storage systems

Assess encryption-at-rest providers' support for PQC. For cloud KMS, ensure ability to rotate and wrap keys with PQ-resistant algorithms. Where the cloud provider is lagging, use client-side PQ wrapping to protect sensitive objects.

7.3 Medical devices and embedded systems

Devices with constrained resources (legacy implants or older scanners) may be unable to accommodate larger PQ keys or heavy computation. For such devices, network-level protections and gateway proxies performing hybrid TLS handshakes or offloading PQ operations are recommended.

8. Mathematical Appendices (selected formal detail)

8.1 KEM construction and hybrid composition

Let $\mathsf{KEM} = (\mathsf{KeyGen}, \mathsf{Encaps}, \mathsf{Decaps})$. For hybrid KEM with classical KEM $K_1$and PQC KEM K_2, compute:

1. $(pk_1, sk_1) \leftarrow \mathsf{KeyGen}_1(1^\lambda)$; $(pk_2, sk_2) \leftarrow \mathsf{KeyGen}_2(1^\lambda)$
2. Sender: $(ct_1, k_1) \leftarrow \mathsf{Encaps}_1(pk_1)$; $(ct_2, k_2) \leftarrow \mathsf{Encaps}_2(pk_2)$
3. Session key: $K = \mathsf{KDF}(k_1 \parallel k_2 \parallel$ context)

Security: if either KEM is IND-CCA secure, and the KDF is a secure extractor, the composed key resists adversaries that break at most one primitive. Formal proofs reduce advantage to break either primitive or KDF properties (Appendix B provides a proof sketch).

8.2 LWE parameter guidelines

For a chosen security level κ, choose dimension n, modulus q, and error distribution χsuch that the best known attacks (e.g., BKZ lattice reduction) have cost ≥ 2^κ. Parameter selection is guided by NIST recommendations and specialized tools (Albrecht's estimator). For production, follow NIST's parameter recommendations for targeted security levels.

9. Risk Analysis and Prioritization

We organize assets by a risk score combining value, retention, and exploitability. High priority: PHI archives, genomic raw data, de-identified datasets that could be re-identified, legal or consent records, device firmware images. Medium: transit TLS for patient portals; Low: public website static content. Prioritization informs phased re-encryption and hybrid deployment.

10. Case Study / Example Roadmap (Hypothetical Healthcare System)

A 5-year roadmap for a medium hospital network:

- **Year 0 (Immediate):** governance, inventory, pilot hybrid TLS on external portals.
- **Year 1:** HSM vendor selection and pilots for PQ key wrapping on archives; PQC testing in staging.
- **Year 2–3:** Enterprise rollout for TLS and API endpoints; re-encrypt highest-value archives; deploy crypto-agility libraries for major internal apps.
- **Year 4–5:** Finish device gateway upgrades; decommission vulnerable primitives for internal services; continuous monitoring.

This roadmap maps to recommendations from NIST/NCCoE and industry whitepapers.

11. Evaluations and Benchmarks

We propose a benchmark suite:

- **Latency:** TLS handshake time (cold/warm), median and tail latencies.
- **Throughput:** MB/s for bulk encryption and decryption for imaging datasets.
- **Resource usage:** CPU cycles, memory, and energy for device classes.
- **Failure modes:** fault injection and side-channel testing for signature verification (see SPHINCS+ fault research).

12. Implementation Considerations & Best Practices

- **Vendor SLAs and roadmaps:** include PQC readiness in procurement.
- **Testing and canary deployments:** stage changes in non-critical environments.
- **Documentation & clinician awareness:** ensure minimal disruption to clinical workflows.
- **Legal & compliance reviews:** update policies to reflect cryptographic changes.

13. Limitations and Future Work

- **Parameter evolution:** PQC parameter selections may change as attacks improve; continuous risk management essential.
- **Device constraints:** many legacy medical devices lack upgrade paths; research into secure gateway patterns remains active.

- **Standards maturation:** as NIST finalizes additional algorithms, guidance must be revisited.

14. Conclusion & Recommendations

Healthcare organizations should treat PQC migration as an enterprise-level program. Key recommendations:

1. **Start now with inventory and governance.**
2. **Deploy hybrid PQC for external TLS endpoints as early pilots.** IETF Datatracker
3. **Protect long-term archives and high-value secrets first.**
4. **Adopt cryptographic agility layers and plan HSM upgrades.**
5. **Coordinate with vendors and cloud providers; require PQ readiness.**

References

1. Fatunmbi, T. O. (2022). Leveraging robotics, artificial intelligence, and machine learning for enhanced disease diagnosis and treatment: Advanced integrative approaches for precision medicine. *World Journal of Advanced Engineering Technology and Sciences*, 6(2), 121–135. https://doi.org/10.30574/wjaets.2022.6.2.0057
2. Fatunmbi, T. O. (2024). Predicting precision-based treatment plans using artificial intelligence and machine learning in complex medical scenarios. *World Journal of Advanced Engineering Technology and Sciences*, 13(1), 1069–1088. https://doi.org/10.30574/wjaets.2024.13.1.0438
3. Fatunmbi, T. O. (2022). Quantum-Accelerated Intelligence in eCommerce: The Role of AI, Machine Learning, and Blockchain for Scalable, Secure Digital Trade. *International Journal of Artificial Intelligence & Machine Learning*, 1(1), 136–151. https://doi.org/10.34218/IJAIML_01_01_014
4. NIST. (2024). *NIST Releases First 3 Finalized Post-Quantum Encryption Standards* (news release). National Institute of Standards and Technology. (NIST’s PQC project and finalized algorithms). NIST
5. NIST Computer Security Resource Center. Post-Quantum Cryptography Standardization Project. https://csrc.nist.gov/projects/post-quantum-cryptography. NIST Computer Security Resource Center
6. SaberiKamarposhti, M., et al. (2024). *Post-quantum healthcare: A roadmap for cybersecurity.* (Paper discussing PQC approaches in healthcare). (Available via PMC). PMC
7. NCCoE / NIST. (2021). *Migration to Post-Quantum Cryptography (project description and guidance).* (NCCoE migration document). NCCoE

8. Campagna, M., & Crockett, E. (IETF Draft). *Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security.* (Hybrid TLS design). IETF Datatracker

9. Bernstein, D. J., et al. (2015). *SPHINCS+: Submission to NIST's Post-Quantum Signature Project.* (Hash-based signatures specification and security analysis). sphincs.org

10. Weger, V., et al. (2022). *A Survey on Code-based Cryptography.* arXiv. (Discusses McEliece family, code-based approaches). arXiv

11. Sun, Z., et al. (2024). *A new McEliece-type cryptosystem using Gabidulin-like constructions.* (Code-based cryptography advances). ScienceDirect

12. Montenegro, J. A., et al. (2025). *A performance evaluation framework for post-quantum TLS.* (Journal article evaluating traditional, hybrid and PQ modes). ScienceDirect

13. Arfaoui, S., et al. (2025). *Systematic review of lattice-based cryptography algorithms.* (Review paper). iacis.org

14. Zafar, A., et al. (2025). *Integrating code-based post-quantum cryptography into TLS.* (Springer paper hybrid framework). SpringerLink

15. Mastercard. (2025). *Migration to post-quantum cryptography White Paper.* (Industry whitepaper advising migration timing and approaches). Mastercard

16. ResearchGate / 2025. *Post-Quantum Migration Strategies: A Hybrid Approach to Cryptographic Transition.* (Research article on hybrid approaches). ResearchGate

17. Kannwischer, A., et al. (2018). *Practical Fault Injection Attacks on SPHINCS.* (Security analysis for hash-based signatures). Kannwischer

18. Albrecht, M. et al. (various). *Parameter selection and LWE security estimates* (use Albrecht estimator and associated literature for parameter selection). (Cite: Albrecht et al., papers on LWE security; include in final manuscript bibliography as needed.)

19. Montenegro, J. A., et al. (2025). *Performance evaluation frameworks for PQC in cloud and TLS.* (duplicate listed for emphasis on performance see #12). ScienceDirect

20. Research paper: *Towards Quantum Resilience: Data-Driven Migration* (arXiv, 2025) provides decision frameworks and metrics for migration planning. arXiv

21. NCSC. (UK). (Whitepaper) *Next steps in preparing for post-quantum cryptography* practical guidance for system owners. NCSC