Q-Day vs FDA-Day: Modelling Post-quantum Readiness Gaps in Long-Lifecycle Healthcare Infrastructure

Danny "Danhammer" Hetzel[1,2], **Calvin Obermeyer**[1] **and Xavier-Lewis Palmer**[1,3]
[1]Biohacking Village, USA
[2]Husaria Security LLC, USA
[3]BiosView Labs, USA

danny@hetzelsecurity.com (Corresponding Author)

Abstract: Healthcare infrastructure constitutes a notably non-agile cryptographic environment, where critical systems rely on legacy devices, unsupported operating systems, and vendor-locked platforms. While contemporary post-quantum security discourse disproportionately prioritizes theoretical cryptanalytic breakthroughs and generic migration strategies, it frequently overlooks the operational reality that healthcare systems cannot meaningfully rotate trust mechanisms within required timelines. This paper addresses this deficit by introducing a specialized healthcare-focused post-quantum readiness framework designed to evaluate cryptographic exposure across diverse vectors, including Picture Archiving and Communication Systems (PACS), DICOM imaging workflows, Internet of Medical Things (IoMT) ecosystems, firmware signing, hospital PKI deployments, VPN architectures, and cloud-connected archival systems. Particular analytical attention is directed toward environments where operational lifecycles routinely surpass the lifespan of their original cryptographic assumptions, thereby creating significant security vulnerabilities. A central theme of this research is the critical application of "harvest now, decrypt later" (HNDL) threat models specifically within medical imaging ecosystems. Unlike ephemeral commercial telemetry, diagnostic imaging studies and longitudinal patient archives possess enduring clinical, legal, and intelligence value, rendering encrypted medical data intercepted today strategically susceptible long after current cryptographic protections become computationally obsolete. This paper asserts that healthcare's post-quantum challenge is fundamentally structural rather than solely cryptographic; regulatory recertification requirements, vendor fragmentation, hardware replacement timelines, and clinical uptime expectations collectively impose operational constraints that render rapid cryptographic agility unfeasible. Consequently, the analysis indicates that healthcare organizations may struggle to transition cryptographic trust models at the speed anticipated by broader enterprise security planning, creating a prolonged exposure window for critical systems. By focusing on the operational risks of the post-quantum migration gap, this research provides a structured method for assessing those systemic constraints.

Keywords: Post-quantum cryptography, Medical-device cybersecurity, Cryptographic agility, PACS, DICOM, Healthcare infrastructure

1. Introduction

Medical devices within the United States fall into a specialized, highly regulated environment that lowers cryptographic agility and slows development lifecycles. Due to patient safety concerns, the regulation affects the speed of commercialization, and the nature of medical device connectivity and application patching is not comparable to the frequency of enterprise environments (Harkin et al., 2024). Together, these constraints can stretch medical-device patching timelines into annual or multi-year intervals, with one empirical study of connected medical-device security updates finding deployment frequencies ranging from once every two months to once every three to four years (Kustosch et al., 2025).

Medical device lifecycles include acquisition, utilization, maintenance, replacement, and retirement, so security changes must fit into a broader lifecycle-management process. Moving a new medical device from concept to market can take approximately three to seven years (Van Norman, 2016). The medical device development ecosystem includes engineering, clinical validation, regulatory review, commercialization, and postmarket considerations (Holmes et al., 2024). Once deployed, high-risk medical devices can remain in service for more than a decade (Harkin et al., 2024). Published lifecycle estimates include approximately 13 years for anesthesia machines, 14 years for defibrillators, 16 years for heart-lung machines, and 13 years for ventilators (Seo et al., 2022). It is not cybersecurity alone that drives this need; rather, it is affected by clinical utility, maintenance costs, part availability, safety risk, and procurement constraints within the organizations. This may result in hospitals and clinics maintaining cryptographically obsolete devices in use.

The extended life cycles create a mirage of an available adaptation window for the pre-Q-Day adaptation interval. This false sense of available reaction time has increased by the progressively narrowing Q-Day timeline (Moody et al., 2024; Mosca and Piani, 2019; Scholten et al., 2024; Hopkins, 2026). NIST's draft post-quantum transition plan proposes migration away from quantum-vulnerable public-key cryptography before those algorithms are deprecated and ultimately removed from federal standards (Moody et al., 2024).

1.1 Goals of this Work and Problem to Address

This paper does not focus on speculative claims about quantum algorithms or the generalized future of cryptanalysis. Instead, it examines the operational risks created by the post-quantum migration gap: where quantum-vulnerable public-key mechanisms are used; whether affected systems can be inventoried and upgraded; whether vendors continue to support the relevant devices and software; whether clinical or regulatory constraints delay deployment; and whether encrypted medical data remains valuable long enough to create harvest-now, decrypt-later exposure (Moody et al., 2024). The post-quantum transition should therefore be treated not merely as a modernization effort, but as a systems-engineering, regulatory, and lifecycle-management problem. The paper focuses on the gap between Q-Day, when a cryptographically relevant quantum computer can practically compromise vulnerable public-key cryptography, and FDA-Day, the point at which FDA regulation requires affected medical devices and healthcare technologies to transition.

The problem is that these two timelines are not synchronized. Cryptographic standards can move quickly once a threat model becomes accepted, but healthcare systems often move through clinical validation, maintenance windows, procurement cycles, and regulatory review before technical changes can be deployed. The relevant question is not only when quantum-capable adversaries may threaten existing public-key cryptography, but whether healthcare organizations can transition before such capabilities are made manifest. Public-key cryptography is not isolated in one place. It appears in TLS connections, VPNs, certificate chains, firmware-signing processes, device authentication, remote vendor access, imaging systems, DICOM workflows, PACS platforms, HL7 implementations, and more.

Q-Day is generally defined as the point at which a cryptographically relevant quantum computer can practically compromise public-key cryptographic systems that would remain infeasible to attack using classical computing (Moody et al., 2024). This definition avoids assigning a fixed calendar date to an uncertain technical milestone and instead focuses on the operational consequence of that capability. FDA-Day is introduced in this paper as the point at which the FDA through regulation requires affected medical devices and healthcare technologies to transition away from quantum-vulnerable cryptography. Following FDA-Day, Medical Device Manufacturers and healthcare organizations may still need to identify cryptographic dependencies, obtain applicable vendor support, complete any regulatory review, deploy changes within clinical environments, and retire obsolete components (FDA, 2016; Harkin et al., 2024; Kustosch et al., 2025; Seo et al., 2022) .

The central focus of this study is that healthcare's post-quantum risk is structural in the development process rather than solely a cryptographic issue, as such Healthcare has less time to prepare for post-quantum mitigations than is commonly assumed. The availability of replacement algorithms does not guarantee that regulated clinical systems can be upgraded, validated, deployed, or replaced within the required timeframe for quantum-vulnerable mechanisms become unsafe (Harkin et al., 2024; Kustosch et al., 2025; Seo et al., 2022). To evaluate this narrowing window, the study introduces a readiness framework designed for PACS and DICOM imaging workflows, Internet of Medical Things ecosystems, hospital PKI, and firmware-signing infrastructure. The framework is illustrated through a PACS/DICOM system-class assessment. The framework aims to assess cryptographic dependency, asset visibility, upgradeability, vendor support, validation requirements, clinical deployment constraints, and expected replacement timelines.

2. Methodology and The Proposed Post-quantum Readiness Framework

Building upon the identified challenges in reconciling clinical lifecycle constraints with emerging quantum threat models, this study introduces the N.I.M.R.O.D. assessment framework. Designed specifically for the healthcare sector, N.I.M.R.O.D. stands for Networked Infrastructure Migration Readiness, Operational Constraints, and Dependencies and is operationalized through six assessment steps: Name the system boundary, identify vulnerable algorithms, Map the cryptographic function, Review vendor support and validation requirements, Observe operational and clinical deployment constraints, and Determine the migration outcome and expected replacement timeline.

This framework addresses the critical observation that cryptographic availability does not guarantee operational transition readiness. Standard post-quantum algorithms are necessary but insufficient in an environment where transition success relies on identifying dependencies, navigating regulatory validation, and managing vendor-controlled lifecycles (Moody et al., 2024; Kustosch et al., 2025). The migration window, defined here as the interval before quantum-vulnerable cryptography becomes untenable due to Q-Day risks or regulatory deprecation, is frequently compressed by legacy platform dependencies, vendor fragmentation, and clinical uptime mandates (Office of Management and Budget, 2022; Harkin et al., 2024; Seo et al., 2022).

The subsequent application of N.I.M.R.O.D. leverages these assessment steps to determine whether a given system possesses a credible migration path, remains tethered to future vendor action, requires substantial infrastructure overhaul, or necessitates complete replacement. By applying this methodology to critical environments such as PACS, DICOM imaging workflows, and hospital PKI ecosystems, this research demonstrates that the post-quantum challenge is fundamentally structural rather than solely technical.

3. The Post-quantum Readiness Framework Defined

As such, the framework can be used to compare the estimated transition requirements of PACS/DICOM, IoMT, and hospital PKI and firmware-signing infrastructure against the narrowing Q-Day/FDA-Day window (Moody et al., 2024).

3.1 N - Name the System Boundary and Assets

The framework evaluates a complete system, rather than an isolated device or application. A system may include: medical-device hardware, firmware and embedded software, operating systems, clinical applications, network services and protocols, cryptographic libraries, certificates, keys, and trust stores, gateways and supporting servers, vendor-managed services, clinical workflows, or maintenance and replacement processes. A device may not have sufficient coverage for various reasons. Assessing a device alone may not provide sufficient coverage because an imaging modality may rely on a PACS server for secure communications, an IoMT device may rely on a gateway or cloud platform, firmware trust may depend on signing keys controlled by the manufacturer, device authentication may depend on hospital PKI, and remote support may depend on VPNs, certificates, or vendor infrastructure. These numerous dependencies create the need to assess following the entirety of the operation chain.

The assessed medical system should also include the organizations and processes that control whether a transition can occur. Relevant stakeholders include the device manufacturer, healthcare delivery organization, third-party software provider, cloud or managed-service provider, certificate authority, clinical engineering team, information technology and security teams, and regulatory and validation stakeholders. This matters because hospitals and healthcare organizations may operate the system without directly controlling the cryptographic implementation and associated processes (Harkin et al., 2024; Holmes et al., 2024; Kustosch et al., 2025).

For each assessment, the Name step identifies the primary device or application, connected infrastructure, external dependencies, cryptographic trust relationships, responsible owner, supporting vendor, clinical function, and expected support and replacement period, ensuring that the assessment boundary extends far enough to capture any component that could prevent migration. Systems should be evaluated separately when they have a distinct vendor, firmware or software stack, cryptographic implementation, clinical purpose, support lifecycle, regulatory status, or migration path. For example, although a PACS archive and an older imaging modality may support the same clinical workflow, they may require separate readiness assessments. This expanded assessment boundary allows the framework to identify whether migration is blocked by the device itself, supporting infrastructure, vendor action, clinical workflow, validation requirements, or replacement timelines.

3.2 I - Identify Quantum-vulnerable Cryptographic Dependencies

The Identify step determines where quantum-vulnerable public-key cryptography exists, what function it performs, and what other components depend on it. Cryptographic dependency is defined here as the extent to which a healthcare system relies on quantum-vulnerable public-key mechanisms for confidentiality, key establishment, authentication, integrity, or software trust (Moody et al., 2024). The Identify step then records the vulnerable algorithm families present within the system. Figure 1 summarizes the key quantum-vulnerable algorithm families and their primary cryptographic functions.

Quantum-vulnerable algorithm families and primary functions

Quantum-vulnerable algorithm family	Primary function
RSA encryption and digital signatures	Confidentiality, authentication, integrity, and software signing
Elliptic-curve cryptography (ECC)	Digital signatures, authentication, and certificate trust
Elliptic-curve Diffie-Hellman (ECDH)	Key establishment and session-key negotiation
Diffie-Hellman (DH)	Key establishment and secure channel negotiation
Quantum-vulnerable public-key algorithms embedded in certificates or cryptographic libraries	Certificate validation, identity authentication, software trust, and inherited cryptographic dependencies

Figure 1: Quantum-vulnerable algorithm families and their primary cryptographic functions

3.3 M - Map the Cryptographic Function and Implementation

The Map step classifies each dependency by its core function and what it functionally supports. This classification is important because a system may require varying migration paths for encryption, authentication, and signing. The framework must then identify where each cryptographic dependency is implemented as a specific component within the system as a whole. Vulnerable mechanisms may be embedded in medical-device firmware, cryptographic libraries, operating systems, clinical applications, PACS or DICOM services, IoMT gateways, VPN infrastructure, hospital PKI, secure-boot processes, firmware signing systems, or vendor managed platforms. These different implementations can reflect different mitigation approaches or viability. The cryptographic mechanism may determine whether migration can be completed through software updates, configuration, firmware replacement, infrastructure modification, or complete device replacement (Moody et al., 2024).

3.4 R - Review Vendor Support and Validation Requirements

The Review step determines the level of support of the system, controls around the assessed cryptographic implementation, and if third-party controlled components can provide a migration path. It also examines whether the change requires verification, regression testing, clinical validation, or regulatory review. These factors are assessed together because vendor-controlled firmware and validation requirements can delay the release or deployment of security updates even when replacement algorithms are available. Many such considerations can quickly expand scope creep, limiting readiness. (Holmes et al., 2024; Kustosch et al., 2025).

3.5 O - Observe Operational and Clinical Deployment Constraints

The Observe step evaluates the practical conditions under which migrations must be deployed. It considers clinical uptime, maintenance windows, physical access, staffing, backups, ability of rollbacks, implemented redundancy, and coordination with users. These constraints may extend the time gap between a vendor release and a fleet-wide deployment, specifically when devices may require to be updated individually or cannot be removed from service without disrupting or delaying treatment (Kustosch et al., 2025).

3.6 D - Determine the Migration Outcome and Expected Replacement Timeline

The Determine step uses the previous findings to help classify if a system has a credible migration path, depends on future vendor action, requires substantial validation or infrastructure changes, cannot transition without replacement, or cannot be assessed because its cryptographic dependencies are unknown. It then compares the expected migration or replacement period against the Q-Day/FDA-Day window. Device age alone does not determine the outcome; remaining vendor support, component availability, maintenance costs, safety risk, procurement constraints, and many other such variables also affect whether migration or replacement can occur within the available time sensitive window (Harkin et al., 2024; Seo et al., 2022). The resulting NIMROD assessment is used to compare the estimated transition requirements of PACS and DICOM workflows, IoMT ecosystems, and hospital PKI and firmware-signing infrastructure against the narrowing Q-Day/FDA-Day window.

4. Application to PACS and DICOM Workflows

To help illustrate the framework a single class of system will be assessed by the N.I.M.R.O.D. framework. We will focus on PACS and DICOM systems to represent clinical data exchange and long-term storage. Other classes could include IoMT to give examples of embedded, distributed or vendor-controlled systems (Affia et al., 2023; Alif et al., 2026) or PKI and firmware to represent authentication, integrity, and general software trust items. While these systems may overlap, the mitigations and constraints create unique profiles for assessment. After applying to the N.I.M.R.O.D. framework, the results can be used to determine readiness in an objective manner.

4.1 PACS and DICOM Imaging Workflows

PACS and DICOM workflows were selected because they combine long-term clinical data storage with distributed communication among imaging devices, archives, clinical applications, and third-party services. PACS commonly acts as a central coordination point for imaging, DICOM services, HL7-connected workflows, web interfaces, workstations, users, and external parties (Cawthra et al., 2020). The following analysis applies the N.I.M.R.O.D. framework at the system level. It evaluates architectural conditions that commonly affect PACS and DICOM environments but does not assume that every healthcare organization uses the same products, profiles, or deployment.

4.1.1 N - name the system boundary and assets

The boundary of the assessment begins with the primary PACS environment, and the scope extends to every component in the PACS imaging ecosystem, including components that to every component that participates in image exchange, storage, access, authentication, or system trust. This includes imaging systems, PACS and third party archives, diagnostic workstations, clinical viewers, radiology and hospital information systems, DICOMweb services, and support connections for vendors (Cawthra et al., 2020). Components with distinct vendors, operating systems, cryptographic libraries, or lifecycles are assessed separately because the least adaptable component may determine the migration timeline.

4.1.2 I - identify quantum-vulnerable cryptographic dependencies

The Identify step examines RSA, ECDSA, ECDH, finite-field Diffie–Hellman, certificate chains, TLS key establishment, VPN authentication, DICOM object signatures, and firmware- or software-signing mechanisms (Moody et al., 2024). DICOM Conformance Statements provide an initial record of supported profiles, but they must be verified against default deployed configurations, certificates, protocol negotiation, software inventories, and vendor documentation (DICOM Standards Committee, 2026). A component may be compliant with current DICOM profiles and security settings while remaining dependent on quantum-vulnerable public-key mechanisms. This is a case where current DICOM standards have not yet adapted to the possible threat.

4.1.3 M - map the cryptographic function and implementation

The Map step assigns each mechanism to its function, including transport confidentiality, endpoint authentication, certificate validation, object integrity, remote access, secure boot, or software and firmware trust. It then records where the mechanism is implemented and whether it is configurable, software-dependent, firmware-dependent, hardware-dependent, or unknown. The relevant unit of analysis is the end-to-end trust path because upgrading a PACS server provides limited benefit when legacy protocols and pipelines cannot validate the new certificate chain, protocol, or signature formats. This is a case where complete systems can be affected by individual components and complete mapping is essential in finding the weakest link.

4.1.4 R - review vendor support and validation requirements

The Review step determines whether vendors can replace the affected mechanism, preserve DICOM interoperability, distribute timely updates and patches, or support the modified post-mitigation implementation throughout the remaining product lifecycle. The least pliable component might be what pushes the rest of the system past the Q-Day timeline. General vendor support is insufficient unless the vendor retains the source code, build environment, signing infrastructure, testing abilities, and monitoring of third-party dependencies needed to produce a deployable migration release in a functionally agile timeline. Cryptographic changes may also require regression, interoperability, clinical, quality-system, and regulatory evaluation before deployment (FDA, 2026; Kustosch et al., 2025). Unmapped third-party dependencies may therefore prevent mitigation before applicable regulatory or cryptographic deprecation deadlines.

4.1.5 O - observe operational and clinical deployment constraints

The Observe step evaluates whether migration can be deployed without unacceptable disruption to clinical diagnostic imaging services. Maintenance windows, physical access, backups, rollback capability, vendor participation, and compatibility testing may substantially delay fleet-wide deployment (Kustosch et al., 2025). Mixed cryptographic states are likely during transition because removing classical support before older legacy systems are upgraded or patched could disrupt clinical workflows, while inability to mitigate preserves the vulnerable dependency.

4.1.6 D - determine the migration outcome and expected replacement timeline

Each component is classified as migration ready, vendor dependent, infrastructure dependent, resupply or replacement dependent, or an unknown exposure. PACS environments are unlikely to receive a uniform classification because modern services may support varying levels of migration while older legacy systems remain dependent on vendor firmware or complete replacement. Patching and upgrades are not always a viable mitigation. The critical path is therefore the last clinically necessary component that prevents removal of quantum-vulnerable mechanisms, supporting the conclusion that the practical migration window may be shorter than analysis restricted to standards only perspective suggests (Harkin et al., 2024; Kustosch et al., 2025; Seo et al., 2022). The N.I.M.R.O.D. assessment shows that PACS and DICOM environments will not migrate uniformly. Due to environmental variability. Newer archives and DICOMweb services may be updated through software or configuration changes, while older systems may depend on vendor firmware, dependent flows, or require full replacement. These findings describe the system class as a whole and would need to be tested against the actual inventory, configuration, vendor support, and remaining lifecycle of a specific healthcare environment.

5. The "Harvest Now, Decrypt Later" Threat Model

The PACS/DICOM assessment shows that quantum vulnerable protections may remain operational across imaging workflows while migration of proper mitigations are applied across archives, protocols, gateways, or vendor controlled components. This delay creates a confidentiality concern and risk now because adversaries can collect encrypted data before Q-Day and retain it for future decryption (Moody et al., 2024). This strategy is a developing adversary strategy described as "harvest now, decrypt later" (HNDL) and applies to ciphertext data compromised today, whether copied from encrypted storage or intercepted in network traffic, and retained until the protecting public-key mechanism can be defeated (Moody et al., 2024).

Potential collection points include archives, backups, DICOM or DICOMweb communications, cloud storage, and remote-access paths. HNDL applies when captured ciphertext depends on a quantum-vulnerable public-key mechanism for key establishment or key protection. Although the data payload may use symmetric encryption, a recorded session or protected key may become recoverable if its associated RSA, ECDH, or other vulnerable public-key mechanism is later broken (Moody et al., 2024). Plaintext exposure is an immediate confidentiality problem and is not part of the HNDL threat model. Future attacks against digital signatures, device authentication, and firmware trust constitute separate post-quantum risks.

HNDL creates exposure before Q-Day because adversaries can collect data while its cryptographic protection remains secure against current attack methods. Its attractiveness increases as the expected time to decryption decreases, provided that the data retains value. Within N.I.M.R.O.D., the assessment should record where encrypted data can be collected, which public-key mechanism protects it, how long the information must remain confidential, and whether migration can occur before that protection is no longer adequate.

6. Discussion

6.1 Long-Term Strategic Value of Encrypted Medical Data

HNDL matters only when the information remains sensitive or useful beyond the expected lifetime of its current cryptographic protection, however, medical information can stay critical as a form of valuable PHI or PII for many years after capture. Treatment histories, persistent diagnoses, identity information, or other permanently sensitive data about a patient can all create the enticing target for HNDL tactics. Current lifecycle and patching studies do not establish the long-term intelligence, privacy, or coercive value of medical data, as this is inherent in the type of clinical data that is gathered in healthcare (U.S. Department of Health and Human Services, 2024). The relevant risk period is the difference between the data's required confidentiality lifetime and the period for which its current public-key protection can reasonably be trusted (Moody et al.,

2024). N.I.M.R.O.D. should therefore record the expected confidentiality period of the data and compare it with the estimated migration or replacement timeline as this will expose overlap and areas of particular concern.

6.2 Structural Constraints on Cryptographic Agility

The approaching issue Q-day and the complex issues around mitigation manifests more than finding appropriate algorithms for a simple replacement of quantum-vulnerable cryptographic implementations. Rather, even with replacement algorithms, algorithm standardization is only the beginning of the mitigation process. Cryptographic availability does not equate to operational deployability, as those algorithms can be introduced into regulated clinical systems before existing protections become inadequate (Moody et al., 2024). Within healthcare, the alteration of cryptographic methods may require vendor development, software or firmware modification, verification, validation, organizational acceptance, and staged deployment across the installed device fleet (FDA, 2016; Harkin et al., 2024; Kustosch et al., 2025). As figure 2 illustrates, the challenges of medical device lifecycle management create a critical overlap window, wherein new devices entering service must navigate intensifying post-quantum migration pressures alongside standard development and patching timelines.

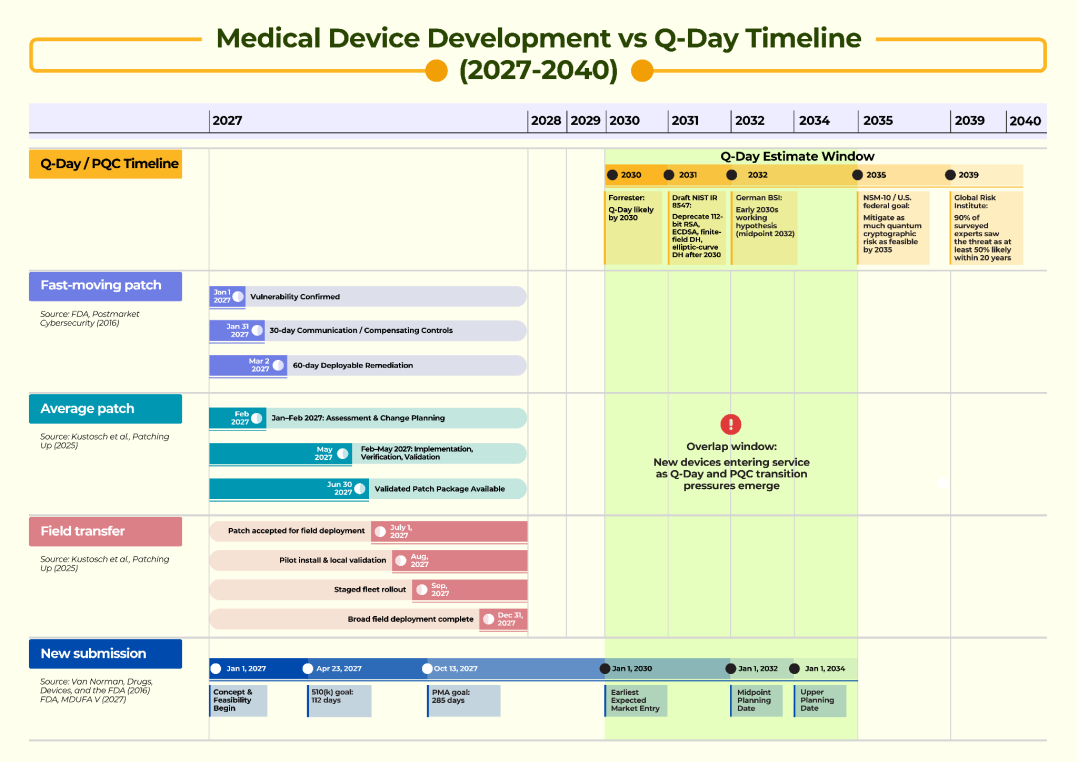
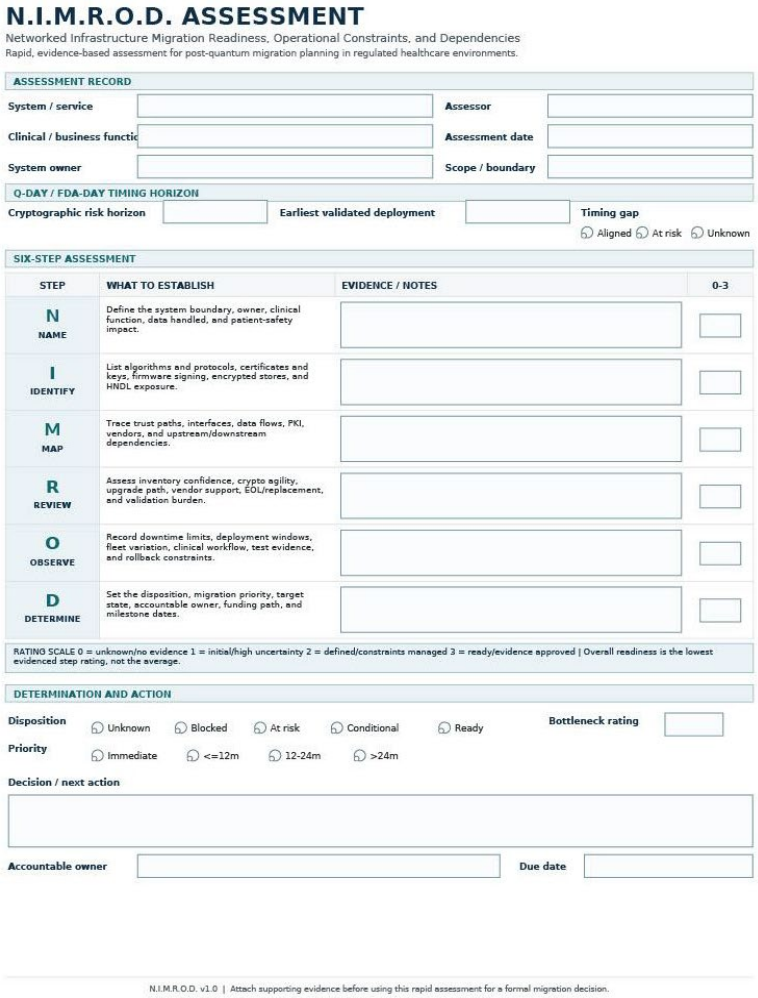


Figure 2: Medical Device Development vs Q-Day Timeline (2027-2040). This figure illustrates the timeline of medical device patching and development against predicted Q-Day milestones, highlighting the critical overlap window where new devices entering service must navigate post-quantum migration pressures

The provided figure illustrates the closing gap in the possible timescales. Emergency remediation may be organized around 30- and 60-day benchmarks, whereas routine patch development and transfer into the clinical field may consume much of a year, and development of a new medical device may extend across three to seven years (FDA, 2016; Kustosch et al., 2025; Van Norman, 2016). The importance of this overlap does not depend on selecting a single Q-Day forecast. A device entering development in 2027 may not reach the market until 2030–2034, when proposed NIST cryptographic deprecation milestones and federal post-quantum migration objectives are already beginning to constrain continued reliance on quantum-vulnerable public-key mechanisms (Moody et al., 2024; Office of Management and Budget, 2022; Van Norman, 2016). The timeline for Q-Day suggests that practical quantum computing could be achieved by 2030.

The structural issues of medical device management and threat mitigation extend past deployment. Some high risk medical devices remain in service for approximately 13–16 years, allowing products designed during the

present transition to remain operational well into the period of post-quantum migration (Seo et al., 2022). Understanding the evolving quantum threat requires continuous assessment of current cryptographic standards and potential attack vectors (Federal Office for Information Security (BSI), 2023). Therefore, the cryptographic adaptability to such threats remains rigid and dependent on the slowest indispensable dependency. Those dependencies could be vendor controlled, a validation process to meet regulations or compliance, interoperability requirements, clinical schedules, deployment and logistical issues (that may be centred around the replacement of the device itself). N.I.M.R.O.D. treats post-quantum readiness as not just a cryptographic component bill of materials to be collected and assessed, but as a development, deployment, lifecycle concern. For those interested, a provisional form for the assessment can be found in Figure 3 below.



N.I.M.R.O.D. ASSESSMENT

Networked Infrastructure Migration Readiness, Operational Constraints, and Dependencies

Rapid, evidence-based assessment for post-quantum migration planning in regulated healthcare environments.

ASSESSMENT RECORD

System / service		Assessor	
Clinical / business functic		Assessment date	
System owner		Scope / boundary	

Q-DAY / FDA-DAY TIMING HORIZON

Cryptographic risk horizon | Earliest validated deployment | Timing gap: Aligned / At risk / Unknown

SIX-STEP ASSESSMENT

STEP	WHAT TO ESTABLISH	EVIDENCE / NOTES	0-3
N NAME	Define the system boundary, owner, clinical function, data handled, and patient-safety impact.		
I IDENTIFY	List algorithms and protocols, certificates and keys, firmware signing, encrypted stores, and HNDL exposure.		
M MAP	Trace trust paths, interfaces, data flows, PKI, vendors, and upstream/downstream dependencies.		
R REVIEW	Assess inventory confidence, crypto agility, upgrade path, vendor support, EOL/replacement, and validation burden.		
O OBSERVE	Record downtime limits, deployment windows, fleet variation, clinical workflow, test evidence, and rollback constraints.		
D DETERMINE	Set the disposition, migration priority, target state, accountable owner, funding path, and milestone dates.		

RATING SCALE 0 = unknown/no evidence 1 = initial/high uncertainty 2 = defined/constraints managed 3 = ready/evidence approved | Overall readiness is the lowest evidenced step rating, not the average.

DETERMINATION AND ACTION

Disposition: Unknown / Blocked / At risk / Conditional / Ready — Bottleneck rating

Priority: Immediate / <=12m / 12-24m / >24m

Decision / next action

Accountable owner | Due date

N.I.M.R.O.D. v1.0 | Attach supporting evidence before using this rapid assessment for a formal migration decision.

Figure 3: The N.I.M.R.O.D form presents a basic template to help guide an assessor through the framework. The lowest score shall be used as the overall score

7. Conclusion

The post-quantum challenge in healthcare necessitates a transition from narrow cryptographic replacement to comprehensive systemic risk management. As shown by the N.I.M.R.O.D. assessment, migration speed is constrained not by algorithm availability, but by the "slowest link" of regulatory, vendor, and clinical dependencies. The collision of narrowing Q-Day timelines and long medical device lifecycles creates an exposure gap that isolated software patches cannot resolve. Organizations must instead prioritize proactive inventory and dependency mapping, specifically addressing "harvest now, decrypt later" threats to sensitive longitudinal data. Ultimately, post-quantum readiness requires shifting security planning to the earliest stages of the development and procurement lifecycle, embedding architectural agility before it becomes impossible to retrofit.

Ethics Declaration: No ethical clearance was required for this work.

AI Declaration: AI tools within Google Docs were used to check grammar and re-organize pre-developed text.

References

Affia, A.-a. O., Finch, H., Jung, W., Samori, I. A., Potter, L., & Palmer, X.-L. (2023). IoT Health Devices: Exploring Security Risks in the Connected Landscape. IoT, 4(2), 150-182. https://doi.org/10.3390/iot4020009

Alif, A., Hasan, K.F., Palaniswamy, B. and Islam, M.M. (2026) 'A framework for post quantum migration in IoT-based healthcare systems', arXiv [Preprint], arXiv:2604.15584v1. Available at: https://doi.org/10.48550/arXiv.2604.15584 (Accessed: 27 July 2026).

Cawthra, J., Hodges, B., Kuruvilla, J., Littlefield, K., Niemeyer, R., Peloquin, C., Wang, S., Williams, R. and Zheng, K. (2020) Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector. NIST SP 1800-24. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.1800-24

DICOM Standards Committee (2026a) Digital Imaging and Communications in Medicine (DICOM), Part 2: Conformance. Available at: https://dicom.nema.org/medical/dicom/current/output/html/part02.html (Accessed: 2 September 2026).

DICOM Standards Committee (2026b) DICOM Standard Status: CP 2573, Update TLS Support to Include Post Quantum. Available at: https://www.dicomstandard.org/cps/ (Accessed: 2 September 2026).

Federal Office for Information Security (BSI) (2023) Security in focus: BSI Magazine 2023/01. Bonn: BSI. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2023-01.pdf (Accessed: 27 July 2026).

Harkin, K.R., Sorensen, J. and Thomas, S. (2024) 'Lifecycle evaluation of medical devices: supporting or jeopardizing patient outcomes? A comparative analysis of evaluation models', International Journal of Technology Assessment in Health Care, 40(1), e2. Available at: https://doi.org/10.1017/S026646232300274X.

Holmes, D.R. Jr, Farb, A., Dib, N., Jacques, L., Rowe, S., DeMaria, A., King, S. and Zuckerman, B. (2024) 'The medical device development ecosystem: Current regulatory state and challenges for future development: A review', Cardiovascular Revascularization Medicine, 60, pp. 95–101. Available at: https://doi.org/10.1016/j.carrev.2023.09.005.

Hopkins, B. (2026) 'Practical quantum computing by 2030 is likely—and so is Q-Day', Forrester Blogs, 11 March. Available at: https://www.forrester.com/blogs/practical-quantum-computing-by-2030-is-likely-and-so-is-q-day/ (Accessed: 27 July 2026).

Kustosch, L., Gañán, C., van Eeten, M. and Parkin, S. (2025) 'Patching up: Stakeholder experiences of security updates for connected medical devices', in 34th USENIX Security Symposium (USENIX Security 25). Seattle, WA: USENIX Association, pp. 2265–2281. Available at: https://www.usenix.org/conference/usenixsecurity25/presentation/kustosch-patching (Accessed: 27 July 2026).

Moody, D., Perlner, R., Regenscheid, A., Robinson, A. and Cooper, D. (2024) Transition to post-quantum cryptography standards. Initial Public Draft, NIST IR 8547 ipd. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.IR.8547.ipd.

Mosca, M. and Piani, M. (2019) Quantum threat timeline report. Toronto: Global Risk Institute in Financial Services. Available at: https://globalriskinstitute.org/publication/quantum-threat-timeline/ (Accessed: 27 July 2026).

Office of Management and Budget (OMB) (2022) Migrating to post-quantum cryptography. Memorandum M-23-02, 18 November. Washington, DC: Executive Office of the President. Available at: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf (Accessed: 27 July 2026).

Scholten, T.L., Williams, C.J., Moody, D., Mosca, M., Hurley, W., Zeng, W.J., Troyer, M. and Gambetta, J.M. (2024) 'Assessing the benefits and risks of quantum computers', arXiv [Preprint], arXiv:2401.16317v2. Available at: https://doi.org/10.48550/arXiv.2401.16317 (Accessed: 27 July 2026).

Seo, G., Park, S. and Lee, M. (2022) 'How to calculate the life cycle of high-risk medical devices for patient safety', Frontiers in Public Health, 10, 989320. Available at: https://doi.org/10.3389/fpubh.2022.989320.

U.S. Department of Health and Human Services (HHS) (2024) The HIPAA Privacy Rule. Available at: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (Accessed: 27 July 2026).

U.S. Food and Drug Administration (FDA) (2016) Postmarket management of cybersecurity in medical devices: Guidance for industry and Food and Drug Administration staff. Silver Spring, MD: FDA. Available at: https://www.fda.gov/media/95862/download (Accessed: 27 July 2026).

U.S. Food and Drug Administration (FDA) (2026) Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions. Silver Spring, MD: FDA. Available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-management-system-considerations-and-content-premarket (Accessed: 2 September 2026).

Van Norman, G.A. (2016) 'Drugs, devices, and the FDA: Part 2: An overview of approval processes: FDA approval of medical devices', JACC: Basic to Translational Science, 1(4), pp. 277–287. Available at: https://doi.org/10.1016/j.jacbts.2016.03.009.