QUANTUM SECURITY LABS

Quantum Risk Executive Briefing

Healthcare Quantum Readiness Assessment

Metro General Hospital

January 10, 2026

Prepared by:

Quantum Security Labs

Executive Summary

CRITICAL RISK

Metro General Hospital's assessment reveals CRITICAL quantum risk exposure with a score of 78/100. Your organization faces serious vulnerabilities across multiple dimensions including data retention policies, cryptographic awareness, and migration readiness. The combination of long-term data retention requirements in healthcare and your current security posture creates an urgent situation. Patient records encrypted today could be harvested and decrypted once quantum computers become capable. Immediate action is required to begin remediation efforts and develop a comprehensive quantum migration strategy.

Key Findings

- Overall quantum risk score: 78/100 (CRITICAL)
- Organization size: Large Hospital/Small System (250,000 - 1,000,000 patients)
- Top vulnerability: Data Retention & Encryption Review
- Recommended action timeline: Immediate

Risk Profile Analysis

Overall Risk Score: 78/100

CRITICAL RISK

Vulnerability Breakdown

#1

DATA RETENTION

How long does your organization retain patient records?

10/10

Critical

#2

MIGRATION READINESS

Has your organization inventoried its current cryptographic systems?

10/10

Critical

#3

LEGACY SYSTEMS

What percentage of your critical systems are more than 10 years old?

10/10

Critical

The Quantum Computing Threat to Healthcare

What is the Quantum Threat?

Quantum computers leverage quantum mechanical phenomena to solve certain mathematical problems exponentially faster than classical computers. This includes the mathematical problems that underpin today's most common encryption methods—RSA, ECC, and Diffie-Hellman key exchange. When sufficiently powerful quantum computers become available, they will be able to break these encryption methods in minutes rather than the billions of years required by classical computers.

Why Healthcare is Uniquely Vulnerable

Healthcare organizations face heightened quantum risk due to several factors: extended data retention requirements (often 20+ years), the extreme sensitivity of patient health information, complex regulatory compliance obligations, and the irreversible nature of medical data exposure. Unlike financial data that can be changed (credit card numbers, account numbers), medical histories cannot be altered—once exposed, the damage is permanent.

"Harvest Now, Decrypt Later" Attacks

Nation-state actors and sophisticated threat actors are already collecting encrypted data with the intention of decrypting it once quantum computers become capable. This means patient data encrypted today using current methods may already be at risk. For healthcare data with 20-50 year retention requirements, this represents an immediate threat, not a future concern.

The Cost of Inaction

Based on Metro General Hospital's size and risk profile, the following projections illustrate potential financial exposure from a quantum-enabled data breach:

Estimated Direct Breach Cost Investigation, notification, credit monitoring, legal fees	**$79,050,000**
Potential Regulatory Fines HIPAA, state privacy laws, and other regulatory penalties	**$11,857,500**
Reputation & Patient Trust Impact Patient attrition, brand damage, recruitment challenges	**$19,762,500**
Operational Disruption System downtime, recovery, productivity loss	**$7,905,000**
Total Potential Exposure	**$118,575,000**

Estimated records at risk: 500,000 patient records
Average cost per compromised record: $180

Projections based on healthcare industry breach data and organizational size. Actual costs may vary based on specific circumstances.

Priority Recommendations

Based on your assessment results, we recommend focusing on these three priority areas:

1

Data Retention & Encryption Review

IMMEDIATE

Your long-term data retention policies require immediate cryptographic attention.

- !’ Conduct an audit of all data retention periods and encryption methods
- !’ Implement quantum-resistant encryption for newly archived data

2

Cryptographic Inventory & Migration Planning

IMMEDIATE

A complete cryptographic inventory is the foundation of quantum readiness.

- !’ Conduct comprehensive cryptographic discovery across all systems
- !’ Classify cryptographic usage by quantum vulnerability level

3

Legacy System Modernization

HIGH

Aging systems with outdated cryptographic implementations present significant risk.

- !’ Inventory all systems over 10 years old and their cryptographic dependencies
- !’ Prioritize upgrade paths for critical legacy systems

Investment Estimate

For an organization of Metro General Hospital's size and complexity, we recommend budgeting for the following quantum migration phases:

Cryptographic Discovery & Risk Assessment 2-3 months	**$75K - $225K**
Migration Strategy & Roadmap Development 1-2 months	**$50K - $150K**
Quantum-Safe Cryptography Implementation 8-12 months	**$300K - $900K**
Testing, Validation & Compliance Verification 2-3 months	**$75K - $225K**
Total Investment 12-18 months	**$500,000 - $1,500,000**

Return on Investment

Potential cost avoidance: $118,575,000

Investment range: $500,000 - $1,500,000

ROI Multiple: 79x - 237x

- Estimates based on typical healthcare organizations of similar size
- Actual costs may vary based on system complexity and scope
- Phased implementation approach recommended to manage costs
- ROI significantly exceeds investment when compared to potential breach costs

Next Steps: Partnering with QSL

Quantum Security Labs (QSL) specializes in healthcare quantum readiness. Our team of cryptographic experts and healthcare security specialists can guide your organization through every phase of quantum migration.

Our Services

Quantum Risk Deep Dive

Comprehensive assessment of your cryptographic infrastructure and detailed migration roadmap

Cryptographic Inventory Service

Complete discovery and classification of all cryptographic implementations across your enterprise

Migration Planning & Implementation

End-to-end support for transitioning to quantum-safe cryptography

Quantum Security Training

Executive and technical training programs on quantum threats and preparedness

Contact Us

https://quantumsecuritylabs.com

healthcare@quantumsecuritylabs.com

1-800-QSL-SAFE

Schedule Your Deep Dive !’