QUANTUM SHIELD LABS

POST-QUANTUM SECURITY EXECUTIVE BRIEFING

Chesapeake Regional Medical Center

Prepared for: **David Morrison**, CISO

500K	$200M+	2027
Patient Records	Potential Liability	Threat Timeline

Report Date: January 29, 2026
CONFIDENTIAL — FOR INTERNAL USE ONLY

EXECUTIVE SUMMARY

CRITICAL: Your organization faces 'Harvest Now, Decrypt Later' attacks NOW

Chesapeake Regional Medical Center maintains **moderate security** with AES-256 and TLS 1.2 encryption. However, this assessment reveals **significant quantum readiness gaps** that expose the organization to immediate and long-term risks. Nation-state actors are actively harvesting encrypted healthcare data today, waiting for quantum computers to decrypt it.

Risk Summary

Category	Current Status	Risk Level
Data in Transit (TLS 1.2)	100% vulnerable to quantum decryption	CRITICAL
Key Management (HSM)	Requires firmware upgrades for PQC	HIGH
Encryption Inventory	Partial coverage—blind spots exist	HIGH
Vendor PQC Readiness	Not assessed across 26-50 vendors	HIGH
Incident Response	No crypto-specific procedures	MEDIUM

Business Impact

Financial Exposure: A quantum breach of 500,000 patient records = $200M to $1B in liability, regulatory fines, and reputation damage.

ROI of Action: Proactive migration delivers 200:1 ROI vs. emergency response costs.

Priority Actions

- **Immediate (30 days):** Deploy automated cryptographic discovery tools
- **Short-term (90 days):** Complete enterprise-wide encryption inventory
- **Mid-term (12 months):** Implement hybrid encryption on critical systems
- **Strategic:** Establish vendor PQC compliance requirements in all contracts

QUANTUM RISK ASSESSMENT

1. Cryptographic Failure Scenario

Your **AES-256** for data at rest is quantum-resistant. However, **TLS 1.2** handshakes using RSA/ECC are 100% vulnerable to Shor's algorithm. A quantum computer breaks these completely—not just weakens them. Your HSMs need firmware upgrades for NIST post-quantum standards, and attackers could forge signatures to alter records or manipulate devices.

2. Why Your 5-10 Year Timeline is Dangerous

Waiting to start migration ignores healthcare's unique constraints

Factor	Reality	Your Risk
Migration Time	3-4 years for orderly transition	If you wait, protection arrives 2032+
Q-Day Estimates	Experts predict 2027-2030	Records exposed before migration completes
HIPAA Retention	50+ year confidentiality required	44-year exposure window for today's data
Retroactive Fix?	PQC cannot protect already-encrypted data	Current records remain permanently exposed

3. Harvest Now, Decrypt Later (HNDL) Threat

Assume your **100,000-500,000 patient records** are being harvested NOW by nation-state actors. Medical data never expires—genetic markers, mental health diagnoses, and chronic conditions remain valuable for blackmail and fraud for the patient's entire life plus 50 years.

HNDL Attack Pattern:

1. Adversaries passively intercept encrypted traffic (completely undetectable)
2. Data archived in long-term storage awaiting quantum computers
3. Once quantum capability arrives, ALL historical data is decrypted simultaneously
4. Mass exposure occurs with no warning until records appear on dark web

4. Encryption Inventory Blind Spots

Your partial inventory and spreadsheet tracking create critical gaps. Security audits typically discover that **40-60% of data stores** are not encrypted as assumed. Your quantum safety is limited by your **slowest vendor**—and you haven't assessed any of them for PQC readiness.

Blind Spot	Discovery Method	Typical Finding
Undocumented encryption	Automated ACDI scan	40-60% gaps found
Vendor dependencies	Supply chain assessment	Weakest link exposure
Shadow IT systems	Network discovery	Unauthorized weak crypto
Integration points	Data flow mapping	Unprotected handoffs

NIST PQC STANDARDS & TECHNICAL REQUIREMENTS

NIST finalized post-quantum cryptography standards in **August 2024**. These are now mandatory for federal systems and will become the healthcare compliance baseline. Organizations should begin migration immediately.

NIST PQC Standards Overview

Standard	Purpose	Replaces	Healthcare Application
FIPS 203 (ML-KEM)	Key Exchange	RSA, Diffie-Hellman	EHR access, VPN tunnels
FIPS 204 (ML-DSA)	Digital Signatures	RSA, ECDSA	Record authentication, updates
FIPS 205 (SLH-DSA)	Backup Signatures	Algorithm diversity	Long-term document integrity

Your Systems: Vulnerability Assessment

System	Quantum Vulnerability	Risk Level
Cisco AnyConnect VPN	RSA/DH handshakes can be intercepted and broken	CRITICAL
Epic EHR	TLS handshakes use quantum-vulnerable algorithms	CRITICAL
Microsoft 365	Identity verification uses breakable encryption	HIGH
Azure/AWS Cloud	Default key management often uses classical RSA/ECC	HIGH
Legacy Medical Devices	Hardcoded encryption cannot be patched	CRITICAL
IoT Devices (100-500)	Insufficient compute power for PQC algorithms	HIGH

TLS 1.2 Forward Secrecy Gap

Critical Vulnerability: TLS 1.2 with static RSA lacks forward secrecy. If your private key is broken by a future quantum computer, ALL past recorded traffic becomes readable—years of patient data exposed retroactively.

Immediate Action: Upgrade to TLS 1.3 which provides the foundation for hybrid PQC extensions.

Legacy Medical Device Risk

Your 100-500 IoT and medical devices represent your **highest long-term risk**. Many devices stay in service 10-15 years with hardcoded encryption that cannot be updated. PQC algorithms require more processing power than legacy devices can provide.

Device Category	Quantum Risk	Recommended Mitigation
Infusion Pumps	Hardcoded keys, no update path	Network isolation + monitoring
Patient Monitors	Weak TLS, 10+ year lifecycles	Quantum-safe gateway proxy
Imaging Systems	Large data transfers vulnerable	Hybrid encryption wrapper

Lab Equipment	Often forgotten in inventory	Include in CBOM discovery

Migration Framework

Phase	Timeline	Key Activities	Deliverable
Discovery	Months 1-6	Complete cryptographic inventory across all systems	CBOM
Pilot	Months 6-12	Test hybrid crypto on non-critical system	Performance baseline
Infrastructure	Year 2	Update HSMs, implement hybrid encryption	Core systems protected
Ecosystem	Year 3	Full PQC deployment, legacy isolation	Complete migration

Key NIST Deadlines

- **August 2024:** FIPS 203, 204, 205 finalized and available for implementation
- **2027-2030:** Expected window for cryptographically-relevant quantum computers
- **2035:** NIST will deprecate and disallow all quantum-vulnerable algorithms

NIST explicitly states: Healthcare must transition 'much earlier' than 2035

COMPLIANCE & REGULATORY ANALYSIS

HHS Regulatory Direction

HHS is actively modernizing standards through the **HIPAA Security Rule NPRM**. Encryption requirements are being updated to address quantum computing threats. IBM's quantum roadmap shows fault-tolerant systems by end of decade—regulators are preparing accordingly.

HIPAA Security Rule Compliance Gaps

Identified Procedural Risk: Your compliance team is only *sometimes* involved in cryptographic decisions. This creates risk of failing to document the "equivalent alternatives" required by HIPAA when standard encryption isn't used.

Audit Exposure: Annual risk assessments that ignore PQC transition may be found deficient by OCR as quantum threats move from theoretical to practical.

Vendor Management Compliance Gaps

Gap Area	Your Current State	Compliance Risk

Assessment Frequency	Onboarding only	No detection of vendor encryption lapse
Contract Language	Generic security terms	No mandate for quantum-safe methods
Ongoing Monitoring	One-time review for 50 vendors	Systemic HIPAA oversight failure

Cyber Insurance Coverage Analysis

Your $5-10M cyber insurance coverage likely contains significant exclusions that could leave your organization exposed in a quantum-related breach:

Exclusion Category	Risk to Your Organization
Failure to Maintain Standards	Generic vendor language may trigger claim denial
Known Regulatory Shifts	Non-compliance with Security Rule NPRM = coverage exclusion
State Privacy Violations	Multi-state breach may exceed sub-limits by $5-50M+
Cryptographic Failure	Most policies are silent on crypto-specific failures

Regulatory Timeline

- **Now:** HIPAA Privacy Rule updates and Security Rule NPRM response required
- **1-3 Years:** NIST PQC standards incorporated into HHS guidance via OCR
- **End of Decade:** Fault-tolerant quantum requires all ePHI quantum-safe

Immediate Documentation Requirements

- **Quantum-Safe Inventory:** Document all data protected by classical encryption
- **Revised BAA Templates:** Add cryptographic roadmap requirements to vendor contracts
- **IR Plan Updates:** Add crypto compromise and HNDL discovery playbooks
- **Board Documentation:** Record this briefing as evidence of due diligence

STRATEGIC ACTION PLAN & ROADMAP

90-Day Quick Wins

Timeline	Action Item	Cost	Outcome
Days 1-30	Board briefing; update IS policy to include quantum risks	$0	Leadership alignment
Days 31-60	Data classification sprint for top 10% high-risk records	$0	Crown jewels identified

Days 61-90	Deploy ACDI pilot on EHR backup system	$5K-$15K	Discovery baseline

12-Month Strategic Roadmap

Quarter	Focus Area	Key Activities	Success Metric
Q1	Discovery	Expand ACDI enterprise-wide; replace spreadsheets	100% inventory
Q2	Risk Scoring	Apply quantum risk scores to all 500K records	Risk-ranked catalog
Q3	Pilot	Test hybrid crypto on non-critical system	<20% perf impact
Q4	Migration	Begin FIPS 203 upgrade on critical systems	Crown jewels protected

Year 1 Budget Allocation ($500K-$2M available)

Investment Category	Low Estimate	High Estimate	Priority
Professional Services (Assessment/Planning)	$50,000	$155,000	Critical
ACDI Tools & Enhanced Monitoring	$30,000	$85,000	Critical
Pilot System Migration	$40,000	$120,000	High
Staff Training & Certification	$30,000	$80,000	High
Personnel (PM/Security Architect)	$180,000	$230,000	Critical
TOTAL YEAR 1 INVESTMENT	$330,000	$670,000	—

Vendor Management Improvements

- Send PQC readiness questionnaire to all 26-50 vendors with PHI access
- Add quantum security clauses to all contract renewals (deadline: Dec 2026)
- Evaluate Azure/AWS PQC roadmaps for cloud infrastructure alignment
- Establish quarterly vendor security review process (vs. onboarding-only)

Incident Response Integration

To align with your 12-month goal of improved incident response capabilities:

- **Define HNDL as Incident Type:** Add to IR plan with retrospective risk assessment trigger
- **Enhanced SIEM Monitoring:** Alert rules for unusual encrypted traffic capture patterns
- **Retrospective Breach Playbook:** Procedures for when historical data is decrypted
- **Crypto Compromise Runbook:** Response steps for algorithm deprecation scenarios

Key Performance Metrics

Metric	Target Date	Success Criteria
Inventory Coverage	Month 6	100% of cryptographic implementations documented
Crown Jewel Protection	Month 12	Top 20% of records in hybrid/PQC encryption
Vendor Compliance	Month 6	100% of critical vendors have documented PQC roadmaps
Performance Validation	Month 9	<20% performance degradation on migrated systems
Compliance Integration	Month 12	Quantum threat in annual HIPAA Risk Analysis

Executive Dashboard Recommendation: Track these metrics monthly and present to leadership quarterly. Create a "Quantum Readiness Score" combining inventory completion, vendor compliance, and migration progress. This provides board-level visibility into your quantum security posture.

RECOMMENDED NEXT STEPS

Engagement Options with Quantum Shield Labs

Service	Description	Investment	Timeline
Security Playbook	DIY guide with templates and checklists	$197	Immediate
Strategic Assessment	1-2 day expert audit of your environment	$7,500	2-3 weeks
Migration Planning	90-day full engagement with roadmap	$25K-$50K	90 days
Ongoing Advisory	Quarterly reviews and compliance monitoring	$2,500/month	Ongoing

Ready to Take Action?

Michael Bennett, Founder & CEO
Quantum Shield Labs

■ michael@quantumshieldlabs.dev
■ quantumshieldlabs.dev

"Protecting Healthcare from Tomorrow's Threats, Today"

Why Quantum Shield Labs?

- **Healthcare Focus:** Specialized HIPAA compliance + quantum risk expertise

- **Practical Approach:** Actionable roadmaps designed for real-world budgets
- **Regulatory Alignment:** Deep understanding of HHS guidance and NIST evolution
- **Executive Communication:** Board-ready materials that translate technical to business risk

Methodology & Sources

This Executive Briefing was generated using Quantum Shield Labs' proprietary 48-question assessment framework, cross-referenced against authoritative sources including NIST FIPS 203/204/205, HHS HIPAA Security Rule NPRM, IBM Quantum Development Roadmap, and Cloud Security Alliance Quantum-Safe Working Group guidance.

Key Sources Referenced

- NIST FIPS 203, 204, 205 — Post-Quantum Cryptography Standards (August 2024)
- NIST IR 8547 — Transition to Post-Quantum Cryptography Standards
- HHS Office for Civil Rights — HIPAA Security Rule NPRM
- IBM Quantum Development Roadmap — Fault Tolerance Timeline
- Cloud Security Alliance — Quantum-Safe Security Working Group
- Quantum Shield Labs — Post-Quantum Security Playbook for Healthcare

Disclaimer: This Executive Briefing is provided for informational purposes based on information provided by the organization. Recommendations should be validated through detailed technical assessment before implementation. Quantum threat timelines are based on current expert consensus and may change as technology evolves. This document does not constitute legal advice regarding HIPAA compliance or other regulatory requirements.

— END OF EXECUTIVE BRIEFING —