

QUANTUM THREAT INTELLIGENCE REPORT: HEALTHCARE & PHARMACEUTICAL INDUSTRY



THREAT LEVEL: EXTREME | Healthcare/pharma face the **MOST SEVERE** quantum threat across all industries due to permanently sensitive medical/genomic data, complex IT infrastructure, and multi-decade clinical trial timelines coinciding with quantum computer arrival.

CRITICAL FINDINGS:

- **Permanent Sensitivity**
Medical records sensitive 50+ years; genomic data forever identifiable across generations
- **Active HNDL Attacks**
Nation-states harvesting encrypted clinical trials, R&D data, patient information NOW
- **Infrastructure Challenge**
77 SaaS applications average; 500-1,000+ APIs; only 4% encrypt 80%+ cloud data; 27% don't know where data stored
- **Quantum Concern**
59% fear encryption compromise; 68% worried about HNDL; 69% key distribution fears (Thales 2025)
- **Breach Statistics**
\$10.9M average cost (highest industry); 238M US residents affected (2024); 287 days to identify breach
- **Global Mandates**
US federal PQC by 2027; HIPAA quantum updates 2025-2026; EU NIS2 by 2030; GDPR penalties €20M
- **Financial Impact**
\$85-130B industry investment required; \$500B-\$2T potential quantum breach exposure

GLOBAL REGULATORY MANDATES & COMPLIANCE TIMELINE

1.1 | UNITED STATES HEALTHCARE QUANTUM MANDATES

Federal Legislation (Source: <https://www.safelogic.com/compliance/pqc-standards>)

A. Quantum Cybersecurity Preparedness Act (Dec 2022)

- **Scope**
Federal agencies + contractors (Medicare/Medicaid providers, VA hospitals, military medical facilities)
- **Requirements**
Inventory quantum-vulnerable systems; develop PQC migration plans; annual OMB reporting
- **Healthcare Impact**
All federal healthcare IT systems and contractors
- **Timeline**
Initial inventory Q4 2025; migration plans Q2 2026

B. OMB Memorandum M-23-02 (Nov 2022)**– Mandate**

Annual cryptographic inventories through 2035

– Priority

High-Value Assets (patient health information systems, clinical trial databases, genomic repositories)

Source: <https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf>

C. NSA CNSA 2.0 (National Security Systems)**– Jan 1, 2027**

New NSS acquisitions CNSA 2.0 compliant (Defence Health Agency, military hospitals)

– Dec 31, 2025

Existing NSS meets CNSA 1.0 or requests waiver

– 2033

Final mandatory compliance for all system types

– Required Algorithms

ML-KEM (CRYSTALS-Kyber), ML-DSA (CRYSTALS-Dilithium), LMS/XMSS

D. Executive Order 14144 (Jan 2025)**– Trump Administration**

Maintains PQC urgency, streamlines roadmap

– TLS 1.3 Requirement

All federal systems by January 2, 2030

– CISA/NSA Deliverable

Quantum-safe product categories by December 1, 2025

– Healthcare Systems

Must support quantum-safe TLS for health information exchange

HIPAA QUANTUM SECURITY UPDATES (Expected 2025-2026)

Current Status: HIPAA Security Rule requires "addressable" encryption (no explicit quantum requirements yet)

Expected Timeline:**– Q4 2025**

Proposed HIPAA quantum security rule (HHS Office for Civil Rights)

– 2026

Public comment period, finalisation

- **2027-2028**

Phased implementation requirements

- **2030**

Full compliance expected

New Requirements (Anticipated):

- ✓ Mandatory PQC implementation for covered entities storing PHI
- ✓ Business Associate Agreements (BAA) must include quantum security provisions
- ✓ Breach notification updates for quantum compromise scenarios
- ✓ Penalties for quantum-vulnerable systems storing PHI after the deadline

Penalties:

Existing HIPAA framework (\$100-\$50,000 per violation, max \$1.5M/year per violation category) + potential quantum-specific penalties

NIST POST-QUANTUM STANDARDS (Finalised Aug 2024)

- **FIPS 203**
ML-KEM (CRYSTALS-Kyber) - Key encapsulation for data encryption
- **FIPS 204**
ML-DSA (CRYSTALS-Dilithium) - Digital signatures for authentication
- **FIPS 205**
SLH-DSA (SPHINCS+) - Hash-based signatures for long-term security
- **FIPS 206: FN-DSA (FALCON)**
Compact signatures for constrained devices (pending)

Source: <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>

1.2 | EUROPEAN UNION HEALTHCARE & PHARMA MANDATES

Source: <https://digital-strategy.ec.europa.eu/en/policies/quantum-secure>; <https://industrialcyber.co/regulation-standards-and-compliance/eu-begins-coordinated-effort-for-member-states-to-switch-critical-infrastructure-to-quantum-resistant-encryption-by-2030/>

NIS2 Directive (Effective Oct 2024; Member State Implementation Oct 2026)

Covered Healthcare Entities:

- **Essential Entities**
Hospitals, pharmaceutical manufacturers, medical device companies, large clinical labs
- **Important Entities**
Telemedicine providers, health data processors, research institutions, pharmacies

- **Penalties**

Up to €10M or 2% of global annual revenue (whichever is higher) for non-compliance

PQC Implementation Timeline:

- **End 2026**

All Member States begin PQC transition; complete cryptographic asset inventory; national strategy developed

- **2027**

Telemedicine providers, health data processors, research institutions, pharmacies

- **2028-2029**

Deploy hybrid PQC solutions (classical + quantum-resistant)

- **2030**

Critical healthcare infrastructure fully quantum-safe (MANDATORY DEADLINE)

- **2035**

Complete migration for all feasible healthcare systems

Penalties:

Up to €10M or 2% of global annual revenue (whichever is higher) for non-compliance

GDPR Quantum Implications

PQC Implementation Timeline:

- Patient data classified as "special category" under GDPR Article 9

- Quantum decryption of patient data = data breach under GDPR

- Controllers/processors liable for inadequate encryption measures

- "Right to be forgotten" (Article 17) complicated by HNDL attacks (data collected today, decrypted later)

Technical Requirements:

- Technical measures must be "state of the art" (Article 32) - quantum threat redefines adequacy

- Data Protection Impact Assessments (DPIA) must address quantum risk

- Data Protection Officers (DPOs) must understand PQC implications

Financial Penalties:

- Up to €20 million or 4% of global annual revenue (whichever is higher)

- Quantum breach could trigger maximum penalties

- Class action lawsuits from affected patients (GDPR Article 82)

European Medicines Agency (EMA) Guidance:

- Clinical trial data must be quantum-safe for submission
- Drug approval documentation requires PQC protection
- Pharmacovigilance systems quantum-secure by 2028
- Manufacturing process data protected with quantum-resistant encryption
- Good Manufacturing Practice (GMP) updates for quantum security

EU Cyber Resilience Act (CRA) - Effective Dec 2027:

- All medical devices with digital elements must support cryptographic agility
- Manufacturers must provide security updates for the product lifecycle
- Quantum-safe updates mandatory for connected medical devices

1.3 | OTHER MAJOR MARKETS

UNITED KINGDOM

- **NCSC**
Healthcare sector prioritised in PQC migration roadmap
- **NHS Digital**
Leading national implementation across the National Health Service
- **Timeline**
Critical NHS systems by 2028; full migration by 2032
- **MHRA (Medicines and Healthcare products Regulatory Agency)**
PQC mandatory for connected medical devices 2026-2028; Software as Medical Device (SaMD) quantum standards
- **2035**
Complete migration for all feasible healthcare systems

JAPAN

- **Investment**
\$7.4B in quantum technology (2025 announcement)
- **Healthcare Focus**
Genomics research protection, medical AI security

- **PMDA (Pharmaceutical and Medical Devices Agency)**
Developing PQC standards for drug approval systems
- **Timeline**
2027-2029 implementation for regulatory submission systems

Source: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025>

SOUTH KOREA

- **KDCA (Korea Disease Control and Prevention Agency)**
Quantum security initiatives for public health data
- **National Health Insurance Service**
PQC pilot program (2025-2026)
- **Timeline**
2026-2029 phased rollout

INDIA

- **National Quantum Mission**
₹6,003.65 crore (\$800M) budget allocation
- **Healthcare Application**
Telemedicine security, digital health records (Ayushman Bharat), genomic research
- **AIIMS Partnership**
Pilot quantum security programs at All India Institute of Medical Sciences
- **Timeline**
2025-2030 phased implementation
- **Focus**
Indigenous quantum security solutions, satellite-based QKD for remote healthcare

CHINA

- **Aggressive Timeline**
Mandating quantum-safe systems for healthcare data by 2026-2027
- **Investment**
Billions in quantum research, 2,000 km operational quantum network
- **Healthcare Priority**
Traditional Chinese Medicine (TCM) database protection, genomic sovereignty

CANADA

- Health Canada
Updating medical device cybersecurity requirements to include PQC
- Provincial Health
Ontario, Quebec leading quantum security pilots
- Timeline
Critical systems 2027-2029

AUSTRALIA

- ASD (Australian Signals Directorate)
Post-quantum planning guidance since 2023
- TGA (Therapeutic Goods Administration)
Medical device quantum security requirements
- My Health Record
National EHR system quantum migration planning
- Timeline
2026-2030 implementation

HEALTHCARE THREAT LANDSCAPE & ATTACK INTELLIGENCE

2.1 | WHY HEALTHCARE IS THE HIGHEST QUANTUM RISK

Source: <https://www.weforum.org/stories/2025/09/pharma-life-sciences-quantum-threat-cybersecurity/>

World Economic Forum Assessment - Unique Healthcare Vulnerabilities:

Risk Factor	Healthcare Reality	Quantum Threat Impact	Severity
Data Lifecycle	50+ years (lifetime + post-death retention)	Decades of encrypted records become decryptable	CRITICAL
Genomic Data	Permanent, unchangeable identifier	Forever sensitive; affects family generations	EXTREME
Clinical Trials	10-15 year duration (Phase I-IV)	Overlaps with CRQC arrival window (2026-2031)	CRITICAL
R&D Value	\$2.6B average per new drug development	Billions in IP vulnerable to theft	EXTREME

Regulatory	HIPAA, GDPR, and FDA mandatory compliance	Quantum breach = massive penalties + litigation	CRITICAL
National Security	Pandemic response, biodefense research	State-sponsored quantum espionage target	EXTREME
Patient Safety	Medical device control, treatment data	Physical harm potential from compromised systems	CRITICAL

Harvest Now, Decrypt Later" (HNDL) Specific Threat:

- Adversaries collecting encrypted healthcare data TODAY
- Expectation: Quantum computers will decrypt 2026-2031
- Once decrypted, genomic/medical data exposure is PERMANENT and IRREVERSIBLE

2.2 | 2025 HEALTHCARE CYBERSECURITY DATA

Thales Data Threat Report - Healthcare & Life Sciences Edition 2025

Source: <https://cpl.thalesgroup.com/blog/data-security/2025-data-threat-report-healthcare-cybersecurity>

Quantum-Specific Healthcare Concerns:

- 59% of healthcare leaders are concerned about future encryption compromise
- 69% fear problems with quantum-resistant key distribution
- 68% worry about "harvest now, decrypt later" attacks
- 50%+ already prototyping or evaluating post-quantum cryptography
- BUT
Only 50% - means half the industry NOT yet preparing

Healthcare IT Infrastructure Complexity Crisis:

- 77 SaaS applications average per healthcare organisation
- Nearly 2 IaaS platforms average (multi-cloud complexity)
- 500-1,000+ APIs per organisation
 - 33% manage more than 500 APIs
 - 14% juggling over 1,000 APIs
- 5+ data discovery tools used by 59% of firms (conflicting policies, overlapping processes)

- 27% have little or NO confidence in identifying where their data is stored
- Only 4% have encrypted 80% or more of sensitive cloud data
- Only 4% have encrypted 80% or more of sensitive cloud data

Breach Trends - Mixed Picture:

- **2021**
Only 14% of firms had 40%+ staff using MFA
- **2025**
12% report breaches (25-point improvement over 4 years)

However, a Quantum threat could catastrophically reverse this progress

Multi-Factor Authentication (MFA) Success Story:

- **2021**
Only 14% of firms had 40%+ staff using MFA
- **2025**
86% achievement (72-point leap in 4 years)
- **Lesson**
When stakes are clear and urgent, healthcare CAN adapt rapidly

AI Security Emerging Concern:

- 27% in GenAI integration or transformation phases
- 67% cite fast-moving AI ecosystem as their #1 security worry
- 50% of AI security spending from existing budgets; 18% from new allocations
- **Primary Concerns**
Model integrity, data reliability, third-party trust, potential misuse
- **Asymmetry Fear**
Compromise at machine speed, remediation at human pace

Healthcare Breach Cost Statistics (IBM 2024):

- \$10.9 million average cost per healthcare data breach (HIGHEST of any industry)
- 287 days average time to identify a breach
- 80 days average time to contain breach
- 2+ years total lifecycle cost (breach costs persist long-term)

- 238 million US residents affected by healthcare breaches (2024)
- 14 breaches involving 1 million+ records each

2.3 | CRITICAL ATTACK VECTORS

A. ELECTRONIC HEALTH RECORDS (EHR) EXPOSURE

- **Scale**
Billions of patient records globally (Epic, Cerner/Oracle Health, Allscripts, Athenahealth)
- **Sensitivity Duration**
Lifetime + 50 years' post-death (regulatory retention requirements)
- **HNDL Activity**
Active collection of encrypted medical database backups
- **Quantum Impact**
Complete patient medical history exposed (diagnoses, treatments, medications, mental health, substance abuse, genetic predispositions)
- **Consequences**
Identity theft, insurance discrimination, employment impact, social stigma, blackmail potential

B. CLINICAL TRIAL & PHARMACEUTICAL R&D DATA THEFT

- **IP Value**
\$2.6 billion average cost to develop one new drug (Tufts Centre study)
- **Timeline Overlap**
Phase I-IV trials span 10-15 years, overlapping CRQC arrival (2026-2031)
- **Target Data**
Patient outcomes, efficacy results, adverse events, drug formulations, manufacturing processes
- **Competitive Impact**
Years of R&D instantly compromised; competitor gains immediate parity
- **National Security**
Biodefense research, vaccine development, pandemic preparedness exposed
- **Regulatory Risk**
FDA/EMA submissions contain sensitive proprietary data

C. MEDICAL DEVICE & IoT INFRASTRUCTURE COMPROMISE

- **Connected Devices**
Pacemakers, insulin pumps, ventilators, patient monitors, infusion pumps

- **Control Systems**
Surgical robots (da Vinci), imaging equipment (MRI, CT, PET), radiation therapy
- **Quantum Vulnerability**
Device authentication broken; PKI certificates compromised
- **Physical Harm Potential**
Life-threatening manipulation (insulin overdose, pacemaker disruption, ventilator shutdown)
- **Scale**
Billions of connected medical devices deployed globally
- **Regulatory**
FDA medical device cybersecurity guidance insufficient for quantum threats

D. GENOMIC DATABASE BREACHES

- **Permanent Sensitivity**
DNA sequence never changes; forever identifiable
- **Family Impact**
Genetic data reveals information about relatives across generations (siblings, children, parents)
- **Discrimination Risks**
 - Health insurance (pre-existing genetic conditions)
 - Life insurance (genetic disease predisposition)
 - Employment (genetic screening)
 - Social stigma (mental health, addiction susceptibility)
- **Collection Scale**
100+ million genomes sequenced globally (23andMe, Ancestry.com, UK Biobank, All of Us)
- **Research Value**
Pharmaceutical companies, biotech firms target genomic databases for drug discovery
- **HNDL Priority Target**
High-value permanent identifiers being actively collected

E. HOSPITAL INFRASTRUCTURE & BUILDING SYSTEMS

- **Building Management**
HVAC, power systems, physical security, access control
- **Patient Monitoring**
Real-time vital signs, alert systems, nurse call systems

- **Supply Chain**
Medication tracking, inventory management, blood bank
- **Emergency Systems**
Life safety, fire suppression, emergency communications
- **Quantum Risk**
Infrastructure control systems authentication compromised; operational disruption

F. TELEMEDICINE & REMOTE CARE PLATFORMS

- **Rapid Growth**
Telehealth visits increased 38x during pandemic; remaining elevated
- **Video Consultations**
Doctor-patient communication encryption is vulnerable
- **Remote Patient Monitoring**
Wearables, home health devices transmitting data
- **Prescription Systems**
E-prescribing platforms handling controlled substances
- **Quantum Threat**
Real-time communication interception; prescription fraud

G. PHARMACEUTICAL SUPPLY CHAIN

- **Manufacturing**
Batch records, quality control, process parameters
- **Distribution**
Track-and-trace systems (Drug Supply Chain Security Act compliance)
- **Cold Chain**
Temperature-sensitive medication monitoring (vaccines, biologics)
- **Counterfeit Prevention**
Hand authentication systems
- **Quantum Risk**
Supply chain integrity compromised; counterfeit drug insertion

QUANTUM COMPUTING CAPABILITIES & TIMELINE

3.1 | CURRENT STATE (OCTOBER 2025)

Operational Quantum Systems:

- IBM Quantum System Two
1,121 superconducting qubits demonstrated
- Google Willow Chip
Achieving quantum computational advantage
- IonQ Forte
64-qubit trapped-ion commercial systems available
- Rigetti
Cloud-accessible quantum processors
- China
Significant quantum computing research facilities; 2,000 km quantum network operational

3.2 | CRYPTOGRAPHICALLY RELEVANT QUANTUM COMPUTER (CRQC) TIMELINE

Year	Qubit Count	Cryptographic Threat	Healthcare Impact
2025	100–500 qubits	Proof-of-concept attacks; limited practical threat	Research phase; monitoring required
2026	500–1,000 qubits	Specialised encryption breaking is possible	Early EHR system vulnerabilities
2027–2028	1,000–2,000 qubits	RSA-2048 potentially breakable; patient data at risk	Clinical trial data exposure begins
2029–2030	2,000–5,000 qubits	Most current encryption is vulnerable	Widespread genomic database compromise
2031+	5,000+ qubits	Complete cryptographic collapse	Total healthcare system security failure

CRITICAL RESEARCH BREAKTHROUGH:

Recent study (Wei et al., 2022) suggests RSA-2048 could be broken by a quantum circuit with only **372 physical qubits** at a circuit depth of thousands - SIGNIFICANTLY lower than previous estimates of 20 million qubits.

Source: <https://arxiv.org/abs/2212.12372>

Implication:

CRQC arrival timeline potentially ACCELERATED; healthcare organisations have LESS time than previously thought.

3.3 | HEALTHCARE CRYPTOGRAPHIC VULNERABILITIES

Healthcare System	Current Encryption	Quantum Attack Method	Risk Level	Breakage Timeline
EHR Platforms	RSA-2048, AES-256	Shor's + Grover's algorithms	CRITICAL	2027-2029
PACS/ Medical Imaging	TLS/SSL, AES-128	Both algorithms	CRITICAL	2027-2029
HL7/FHIR APIs	OAuth2, JWT (RSA-based)	Shor's algorithm	CRITICAL	2027-2028
Medical Devices	ECC (elliptic curve), AES-128	Both algorithms	EXTREME	2026-2028
Genomic Databases	AES-256, RSA-4096 PKI	Both algorithms	PERMANENT RISK	2028-2030
Clinical Trial Systems	SSL/TLS, RSA-2048	Both algorithms	CRITICAL	2027-2029
Telemedicine Platforms	WebRTC (DTLS-SRTP), RSA	Shor's algorithm	HIGH	2027-2029
Pharmacy Systems	TLS 1.2/1.3, AES-256	Grover's algorithm (partial)	CRITICAL	2029-2031

Quantum Attack Methodologies:

- **Shor's Algorithm**
Efficiently factors large numbers and solves discrete logarithm problems → breaks RSA, ECC, Diffie-Hellman
- **Grover's Algorithm**
Speeds up unstructured search → reduces effective key length by half (AES-256 becomes AES-128 equivalent)
- **Cold Chain**
Temperature-sensitive medication monitoring (vaccines, biologics)

- **Counterfeit Prevention**
Hand authentication systems
- **Quantum Risk**
Supply chain integrity compromised; counterfeit drug insertion

THREAT ACTOR CAPABILITIES & ATTRIBUTION

4.1 | NATION-STATE ACTORS

CHINA

- **Capabilities**
Advanced quantum research; operational quantum network; significant qubit development
- **Healthcare Targets**
Pharmaceutical IP, clinical trial data, genomic research (population health studies)
- **Attribution**
APT groups linked to Ministry of State Security (MSS), PLA Unit 61398
- **HNDL Activity**
Active since 2018+; massive collection of encrypted medical research databases
- **Motivation**
Economic espionage, technology transfer, strategic advantage in biotechnology

RUSSIA

- **Capabilities**
State-sponsored cyber operations; SVR (Foreign Intelligence Service) advanced persistent threats
- **Healthcare Targets**
Biopharma companies, vaccine research, biodefense data
- **Notable Operations**
2023-2024 SVR exfiltrated terabytes from Microsoft corporate email (US government accounts)
- **HNDL Activity**
Collection of pharmaceutical manufacturing data, regulatory submissions
- **Motivation**
Economic gain, disruption of Western pharmaceutical dominance

NORTH KOREA

- **Capabilities**
Cyber-criminal nexus; sophisticated cryptocurrency theft operations
- **Healthcare Targets**
Healthcare ransomware (funding regime), pharmaceutical companies
- **Methods**
Cybercrime for revenue generation (circumvents sanctions); hacking-for-hire
- **Partnerships**
Working with foreign criminal networks as third-party enablers
- **HNDL Activity**
Opportunistic collection for future ransomware campaigns

IRAN

- **Capabilities**
Increased cyberattack sophistication; regional cyber warfare focus
- **Healthcare Targets**
Israeli healthcare institutions, Western pharmaceutical companies
- **Recent Activity**
Escalation of cyberattacks, cyberespionage, information operations
- **Motivation**
Political objectives, regional conflict, economic sanctions circumvention

4.2 | ORGANIZED CYBERCRIME GROUPS

Healthcare Ransomware Operators

- **LockBit, ALPHV/BlackCat, Royal**
Specifically targeting healthcare (highest ransom payment rates)
- **Average Healthcare Ransom**
\$1.5 million+ (healthcare pays 65% of the time due to operational criticality)
- **Quantum Preparation**
Collecting encrypted backups for future decryption and extortion
- **Triple Extortion**
Encryption + data theft + threatening patient notification

Data Brokerage Networks

- **Underground Markets**
Medical records selling for \$250-\$1,000 each (vs \$1-\$2 for credit cards)
- **Genomic Data**
Premium pricing for genetic information
- **Prescription Data**
Valuable for pharmaceutical marketing, insurance fraud

4.3 | CORPORATE ESPIONAGE

Pharmaceutical Competitors:

- **Domestic & International**
Stealing drug formulations, clinical trial results, manufacturing processes
- **Methods**
Insider threats, supply chain compromises, encrypted data collection
- **Value**
Billions of dollars in R&D shortcuts; accelerated time-to-market

Biotech Startups:

- **IP Theft**
Novel therapeutic approaches, gene therapy techniques, personalised medicine algorithms
- **Quantum Opportunity**
Encrypted research communications, patent applications, investor presentations

MITIGATION STRATEGIES & IMPLEMENTATION ROADMAP

5.1 | IMMEDIATE ACTIONS (Q4 2025 - Q1 2026)

A. COMPREHENSIVE DATA MAPPING (Address 27% with no visibility)

- ✓ Identify ALL sensitive data storage locations (PHI, genomic, clinical trials, R&D)
- ✓ Create a detailed data inventory across 77 SaaS applications
- ✓ Document data flows through 500-1,000+ APIs
- ✓ **Priority**
Patient-facing systems, genomic databases, clinical trial platforms
- ✓ **Tool**
Implement unified data discovery platform (consolidate from 5+ tools)

B. CRYPTOGRAPHIC ASSET INVENTORY

- ✓ Audit current encryption implementations across the entire infrastructure
- ✓ Create Cryptographic Bill of Materials (CBOM) - document every algorithm, key, certificate
- ✓ Identify quantum-vulnerable systems (RSA, ECC, DES, legacy TLS)
- ✓ Map dependencies: internal systems, third-party vendors, cloud providers
- ✓ **Compliance**
Required for HIPAA quantum updates, OMB M-23-02, EU NIS2

C. CLOUD SECURITY ENHANCEMENT (Currently only 4% adequate)

- ✓ Encrypt 80%+ of sensitive cloud data (nearly 50% currently sensitive but unprotected)
- ✓ Implement quantum-resistant key management systems
- ✓ Deploy Quantum Random Number Generators (QRNG) for high-entropy keys
- ✓ Conduct cloud security posture assessments
- ✓ **Timeline**
Achieve 80% encryption by Q2 2026

D. API SECURITY HARDENING (500-1,000+ API vulnerability surface)

- ✓ Implement quantum-safe authentication for all APIs
- ✓ Update OAuth2, JWT implementations to use PQC algorithms

- ✓ Monitor API traffic for anomalous encrypted data exfiltration
- ✓ Establish an API gateway with centralised PQC enforcement
- ✓ **Standard**
 - Align with HL7 FHIR quantum security extensions (under development)

E. LEGACY SYSTEM PRIORITIZATION

- ✓ Inventory systems requiring PQC upgrades
- ✓ **Priority Order**
 - (1) Genomic databases, (2) EHR platforms, (3) Clinical trial systems, (4) Medical devices, (5) Administrative systems
- ✓ Identify systems requiring hardware replacement vs software updates
- ✓ Develop sunset plans for systems that cannot be upgraded

F. GOVERNANCE & POLICY

- ✓ Establish C-level quantum security oversight committee
- ✓ Board-level quantum risk reporting (required by EU NIS2)
- ✓ Update incident response plans for quantum breach scenarios
- ✓ Develop quantum security policies and standards
- ✓ **Compliance**
 - Data Protection Impact Assessment (DPIA), including quantum risk

5.2 | SHORT-TERM IMPLEMENTATION (2026-2027)

A. POST-QUANTUM CRYPTOGRAPHY PILOTS (Join 50%+ already evaluating)

- ✓ Deploy NIST-approved algorithms in test environments
 - ML-KEM (FIPS 203): Key encapsulation for EHR, databases
 - ML-DSA (FIPS 204): Digital signatures for authentication, audit logs
 - SLH-DSA (FIPS 205): Long-term signatures for genomic data, clinical trials
- ✓ Measure performance impact (CPU, latency, storage)
- ✓ Test interoperability with existing systems
- ✓ Validate FIPS 140-3 compliance for the US market

B. MEDICAL DEVICE SECURITY TRANSFORMATION

- ✓ Engage manufacturers on quantum-safe firmware updates
- ✓ Update procurement requirements: mandate PQC support for all new devices
- ✓ Prioritise life-critical devices: pacemakers, insulin pumps, ventilators
- ✓ **Timeline**
Critical devices by 2028 (EU CRA requirement, FDA guidance)
- ✓ **Regulatory**
Align with FDA medical device cybersecurity guidance updates

C. EHR PLATFORM QUANTUM MIGRATION

- ✓ Coordinate with Epic, Oracle Health (Cerner), Allscripts, Athenahealth
- ✓ Implement hybrid encryption (classical + PQC) during transition
- ✓ Ensure HIPAA compliance throughout migration
- ✓ Patient data export/import testing with quantum-safe encryption
- ✓ **Timeline**
Begin migration 2026; complete by 2029

D. QUANTUM-RESISTANT KEY MANAGEMENT (Address 69% key distribution concern)

- ✓ Implement enterprise-wide Key Management System (KMS) with PQC support
- ✓ Deploy Quantum Random Number Generators (QRNG) for cryptographic key generation
- ✓ Establish quantum-safe Public Key Infrastructure (PKI)
- ✓ Certificate lifecycle management automation (prepare for 47-day renewal cycle by 2029)
- ✓ **Standard**
Align with NIST SP 800-57 key management guidance (PQC updates)

E. GENOMIC DATA SPECIAL PROTECTION (Permanent sensitivity requires the strongest security)

- ✓ Implement quantum-safe encryption for all genomic databases
- ✓ Consider Quantum Key Distribution (QKD) for the highest-security genomic repositories
- ✓ Strict access controls with quantum-resistant authentication
- ✓ Anonymisation techniques resilient to quantum re-identification attacks

- ✓ **Compliance**

- GDPR Article 9 special category data; genetic non-discrimination laws

F. CLINICAL TRIAL SYSTEM HARDENING

- ✓ **Quantum-safe encryption for patient recruitment, randomisation, and data collection**

- ✓ **Protect statistical analysis plans, interim results, and final reports**

- ✓ **Secure investigator communications, site monitoring data**

- ✓ **FDA/EMA submission portals quantum-safe authentication**

- ✓ **Timeline**

- New trials starting 2027+ must use PQC

G. SUPPLY CHAIN QUANTUM REQUIREMENTS

- ✓ **Update Business Associate Agreements (BAA) with quantum security provisions**

- ✓ **Vendor risk assessments, including PQC readiness**

- ✓ **Procurement contracts mandate quantum-safe compliance timelines**

- ✓ **Third-party security audits verify PQC implementation**

- ✓ **Compliance**

- EU NIS2 supply chain security requirements

5.3 | MEDIUM-TERM TRANSFORMATION (2027-2030)

A. HOSPITAL-WIDE PQC DEPLOYMENT

- ✓ **Roll out quantum-safe encryption across ALL hospital systems**

- ✓ **Electronic Medical Records (EMR), Laboratory Information Systems (LIS), Radiology Information Systems (RIS)**

- ✓ **Pharmacy systems, billing, scheduling, patient portals**

- ✓ **Staff training programs**

- IT administrators, clinicians, compliance officers

- ✓ **Patient communication**

- Data protection enhancements, privacy assurances

B. PHARMACEUTICAL MANUFACTURING PROTECTION

- ✓ **Quantum-safe encryption for batch records, quality control data**

- ✓ **Manufacturing execution systems (MES) with PQC**

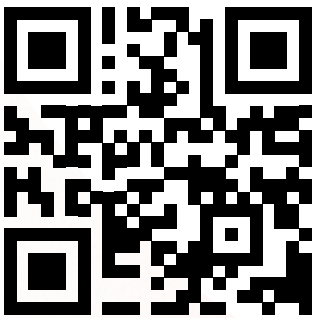
- ✓ Secure supply chain from raw materials to distribution
- ✓ Serialisation and anti-counterfeiting systems quantum-resistant
- ✓ **Regulatory**
 - EU GMP Annexe 11 updates for quantum security

C. HEALTH INFORMATION EXCHANGE (HIE) QUANTUM-SAFE STANDARDS

- ✓ Develop quantum-safe HL7 FHIR implementation guides
- ✓ National/regional HIE infrastructure PQC deployment
- ✓ Cross-border health data sharing with quantum security
- ✓ **Interoperability testing**
 - Ensure quantum-safe systems communicate seamlessly



Tomorrow's **Quantum** **Security, Today.**



Scan for more details

Registered Office:

QuNu Labs Private Limited, Centenary
Building, 2nd Floor, East Wing, #28 MG Road
Bengaluru - 560025

CIN: U72900KA2016PTC096629

India

USA

Australia

Global