IBM Consulting

Quantum Risk in Healthcare and Life Sciences

Securing Healthcare and Life Science Systems in a Post-Quantum World

Umut Cikla
IBM Quantum Safe Asia Pacific Leader
umut.cikla@ibm.com

→ Bring useful quantum computing to the world

→ Make the world quantum safe

Quantum computing is a new way to solve problems that are impossible for classical computers

It introduces unprecedented computational power to bring innovation to many industries.

Developing lighter, longer-lasting batteries for electric vehicles, electronics, and energy grid storage

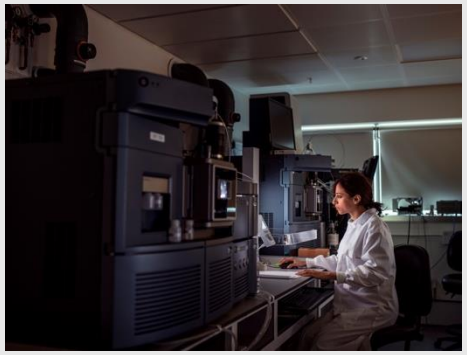
Designing lighter, stronger materials to allow planes to be more efficient and to need less maintenance

Discovering new classes of antibiotics to counter the emergence of multidrug-resistant bacterial strains

Designing optimal superconductors for MRI, electromobility, and renewable energies

Solving algebra in [exponential] spaces. Finding hidden patterns in structured problems.

Improving anomaly detection, as for rare events detection and fraud detection



Improving patient outcomes by designing optimal cell-centric therapeutics

Strengthening risk management through better time series and sequence prediction

Optimising vehicle routing and scheduling for large-scale logistics networks

moderna

Predicting mRNA secondary structures with quantum optimization techniques

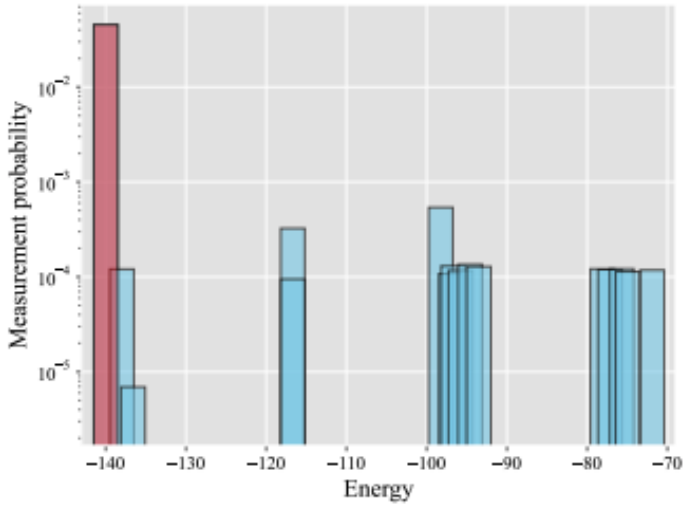
Optimization

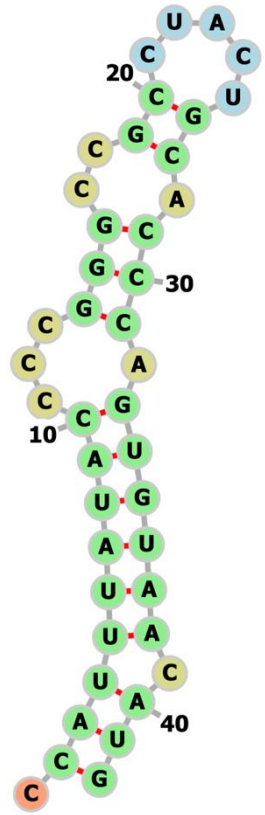
Moderna partnered with IBM to develop quantum computing algorithms for predicting mRNA secondary structures at greater scale and accuracy, with the goal of unveiling novel and more diverse mRNA therapies.

Running the CVaR-VQA algorithm on IBM Quantum Eagle and IBM Quantum Heron processors yielded accurate insights into folding mechanisms for mRNA sequences of up to 42 nucleotides (mapped to 10–80 qubits) and their associated energy states that match the results of the classical solver CPLEX.

"Our world is a quantum mechanical world, and so when we try to simplify things in a deterministic world, we're not going to really be able to emulate that complexity."

Wade Davis
Senior Vice President, Digital for Business, Moderna





These figures show (a) the measurement probability of sampled bitstrings plotted against bitstring energies for the 80-qubit problem, where the red bar indicates the probability corresponding to the lowest energy bitstring; and (b) the optimal folded structure of the 42-nucleotide, 80-qubit mRNA sequence based on the corresponding lowest energy bitstring found by the hardware run.

Read the papers: arXiv:2405.20328; arXiv:2507.18817

Explore the demo: ibm.biz/BdGAB6

Our modern digital world depends on cryptography. It is the ultimate line of defense.

Prime factors	2048-bit composite integer	Expected computation time
= p x q	25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564392120103971228221207203570	The most powerful computer **today:** Millions of years Shor's quantum algorithm: **Hours**

Public key encryption • Digital signatures • Key exchange algorithms

RSA • DSA • ECC • ECDSA • DH

What can a cybercriminal do?

Harvest now, decrypt later

Availability of “cryptographically relevant” quantum computers

Before

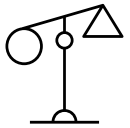
After

“Q-Day”

Harvest confidential data to decrypt later

Decrypt lost or harvested confidential data by breaking encryption

Disrupt business with manipulation through fraudulent authentication



Manipulate digitally signed contracts and legal history by forging digital signatures

Adversaries can for example:

Launch extortion attacks by threatening to disclose harvested data

Create fake identities for websites or system administrators

- Create fake software downloads and software updates
- Create indistinguishable fraudulent land records or lease documents
- Spend Bitcoin

Why Quantum Risk Matters to the Healthcare and Life Science Industry

Healthcare and life sciences organizations hold some of the most sensitive and high-value data in the world — from patient records and clinical trial results to genomic datasets and pharmaceutical IP.

The quantum threat puts this information and the systems that protect it at risk, as today's cryptographic methods will no longer be secure once quantum computers reach sufficient scale

Patient Data Confidentiality

Quantum computing could render current encryption obsolete, exposing sensitive patient health records and personal identifiers to breach, reputational damage, and regulatory fines.

Intellectual Property Protection

Proprietary drug formulas, clinical trial results, and R&D datasets could be decrypted by future quantum adversaries, risking competitive advantage and lost revenue.

Regulatory Compliance Risk

Failure to future-proof cryptography may result in non-compliance with HIPAA, GDPR, FDA, and EMA regulations, creating legal and financial liability.

Clinical Trials and Research Integrity

Quantum-enabled attacks could compromise trial data integrity or authenticity, undermining regulatory approvals and investor confidence.

Supply Chain and Manufacturing Security

Pharmaceutical supply chains, including logistics, drug production, and packaging, are vulnerable to tampering if cryptography is broken, threatening patient safety and operational continuity.

Trust in Digital Health Services

Telemedicine, connected devices, and cloud-based analytics could be intercepted or manipulated, eroding patient trust and market credibility in a sector increasingly dependent on digital channels.

Top 10 Quantum Risk Areas in Healthcare and Life Science

As the healthcare and life sciences sector becomes increasingly dependent on interconnected digital systems—from electronic health records and telemedicine platforms to clinical trial management and global supply chains—the advent of quantum computing poses a fundamental threat to the cryptographic foundations securing these operations.

From protecting sensitive patient data and safeguarding medical devices to ensuring the integrity of clinical trial results and secure collaboration with research partners, nearly every function in the sector relies on cryptographic mechanisms that will be vulnerable to future quantum attacks.

The implications are sector-wide: compromised patient privacy, tampered clinical trial or genomic data, manipulation of research outcomes, and exposure of proprietary drug formulations—potentially undermining safety, regulatory compliance, market trust, and operational continuity.

Electronic Health Records (EHR) Security
→ Patient medical histories and personal identifiers could be decrypted, exposing individuals to identity theft and violating HIPAA/GDPR.

Medical Device Communications
→ Implantable and connected medical devices (e.g., pacemakers, insulin pumps) could be hijacked if quantum attackers break device-to-cloud encryption.

Pharmaceutical Intellectual Property
→ Proprietary drug formulas and trial data could be stolen by decrypting stored or intercepted research files.

Clinical Trials Data Integrity
→ Adversaries could manipulate trial data integrity or authenticity, undermining regulatory approval and public trust.

Genomic and Personalized Medicine Data
→ Massive genomic datasets could be decrypted in the future (“harvest now, decrypt later”), exposing patients to discrimination risks.

Healthcare Payment Systems
→ Quantum attacks could undermine the integrity of payment and insurance claim systems, leading to fraud and revenue loss.

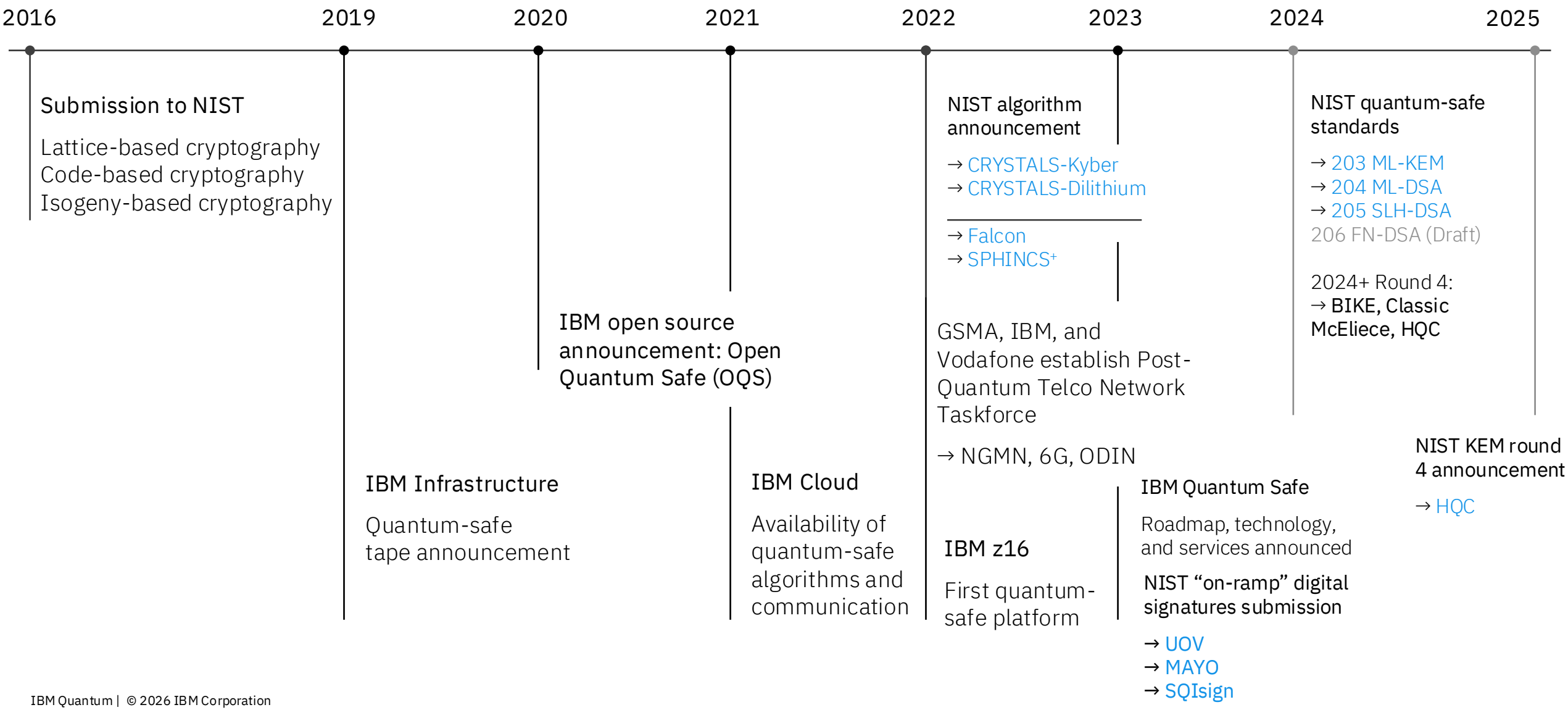
Telemedicine Platforms
→ Video consultations and remote diagnostics could be intercepted, leading to exposure of confidential patient–doctor interactions.

Supply Chain Integrity
→ Compromised cryptographic controls could enable counterfeit drugs or tampered shipments to infiltrate the pharma supply chain.

Regulatory Compliance and Audit Exposure
→ Failure to address quantum threats may create regulatory non-compliance in the future (e.g., FDA, EMA, HIPAA).

Cloud & Research Collaboration Platforms
→ Sensitive cross-border data exchanges (universities, labs, biotech startups) are vulnerable to interception and later decryption.

Launching the era of quantum safe in IBM



Efficiency though industries and ecosystems

Global Guidance

EU
DORA (2025)

UK
NCSC (2023)
Start planning;

Netherlands
AIVD (2023)
Start planning;

Germany
BSI (2022)
Start planning;

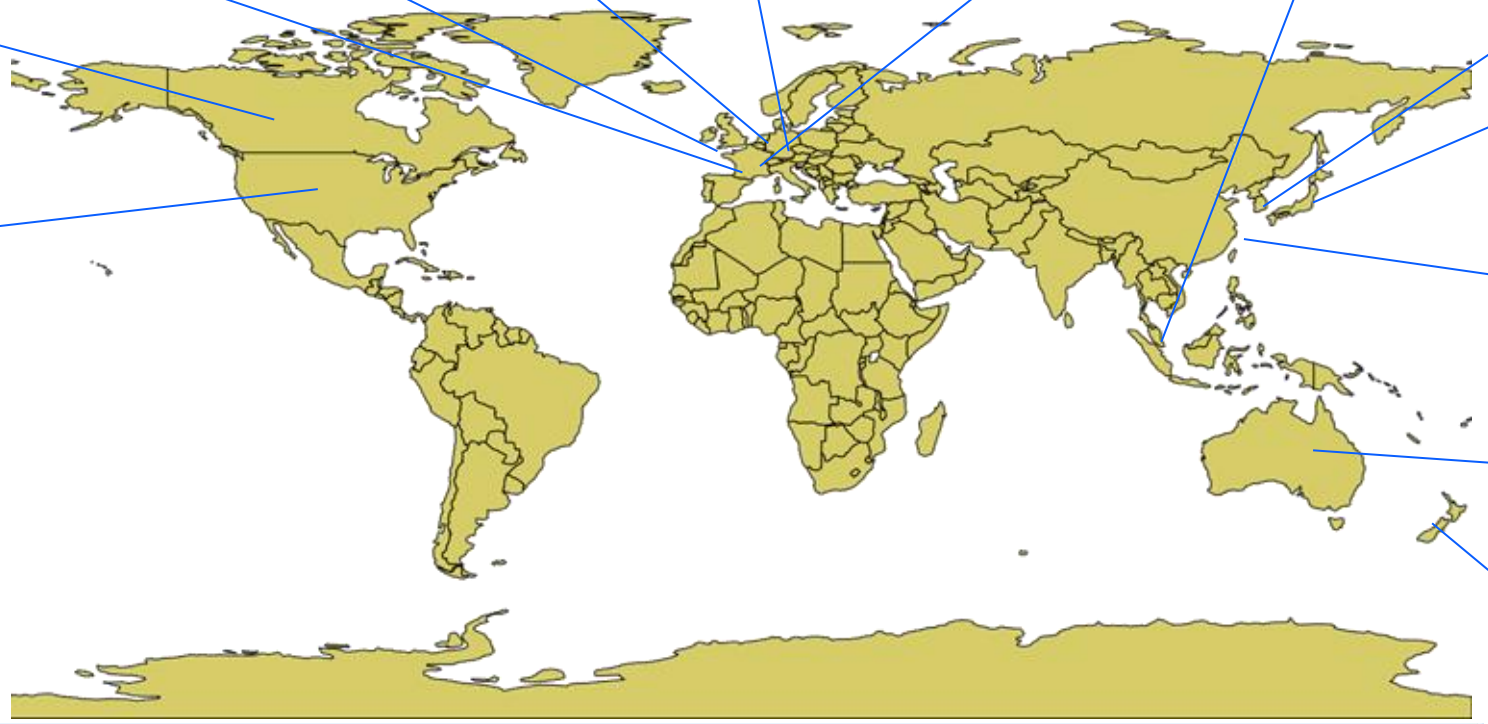
France
ANSSI (2022)
Start planning;
Transition from 2025

Singapore
MCI (2022)
Monitoring NIST

S. Korea
MSIT (2022)
Start competition 1st round (Nov.'22-Nov.'23)

CANADA
Cyber Centre (2023)
Start planning; impl. from 2025

USA
NSA (2022)
Implementation 2023-2033



Japan
CRYPTREC
Start planning; initial timeline

China
CACR (2020)
Start Planning

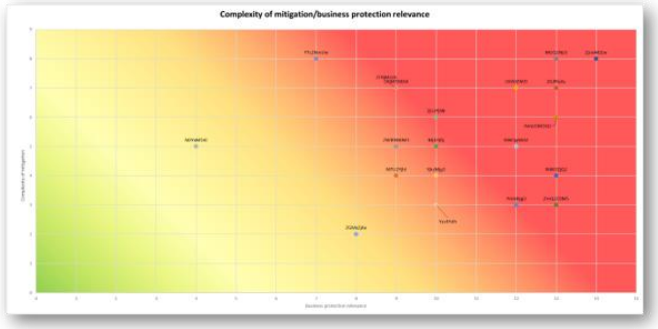
Australia
ASD (2023)
Nat'l Strategy (2023)

New Zealand
Start Planning
NZISM (2022)

MITRE · GSMA · NCCoE National Cybersecurity Center of Excellence · IETF · World Economic Forum · PCI DSS Compliant · MAS Monetary Authority of Singapore · Post-Quantum Cryptography Alliance

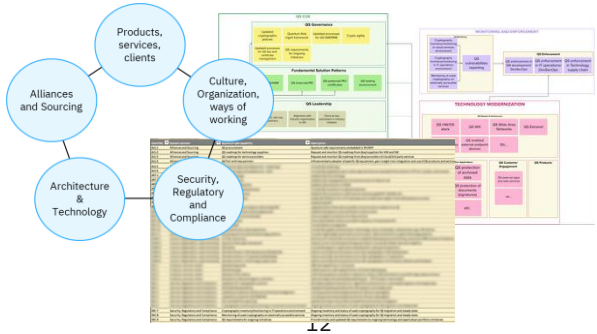
IBM Quantum Safe approach

Execute an end-to-end quantum-safe transformation with a clear target date while establishing crypto-agility.



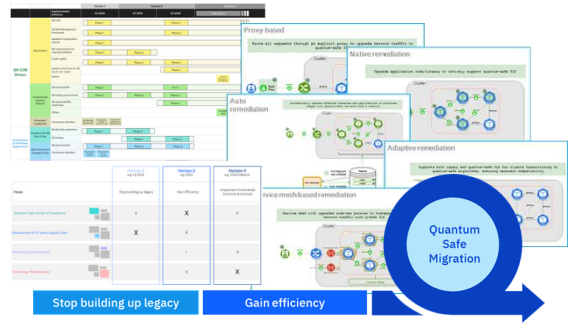
Develop a quantum-safe transformation strategy

- Quantum-safe understanding
- Map affected assets and their dependencies
- Identify potential urgent actions
- Outline next steps



Discover cryptographic usage and analyze risk posture

- Identify quantum safe-related capabilities (target state)
- Prioritize actions and initiate urgent measures
- Define implementation approach and governance

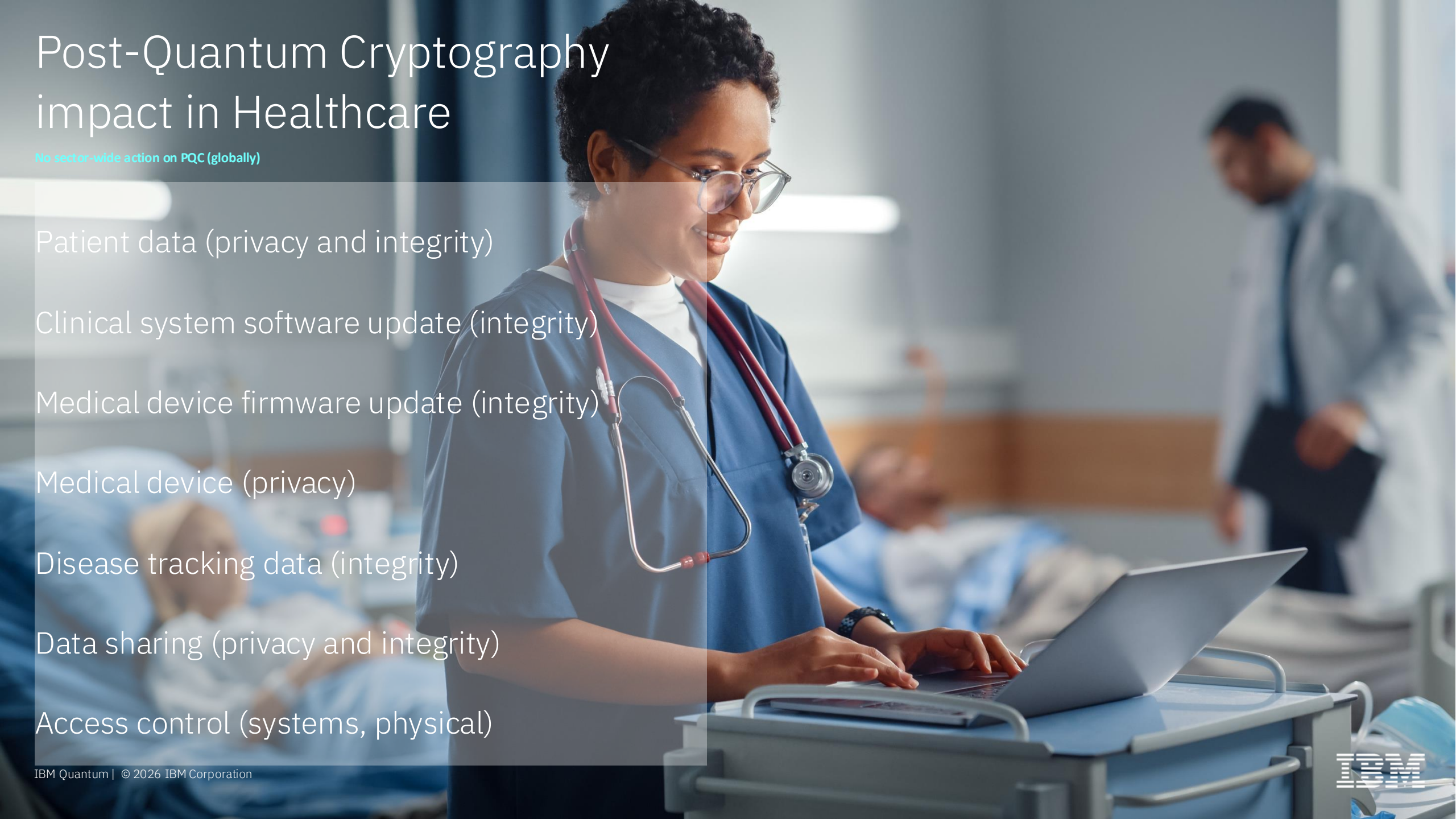


Remediate vulnerabilities and build crypto-agility

- Implement actions aligned with internal initiatives, and ecosystem
- Apply predefined and validated patterns and artifacts
- Monitor technology progress and adjust approach

Post-Quantum Cryptography impact in Healthcare

No sector-wide action on PQC (globally)



Patient data (privacy and integrity)

Clinical system software update (integrity)

Medical device firmware update (integrity)

Medical device (privacy)

Disease tracking data (integrity)

Data sharing (privacy and integrity)

Access control (systems, physical)

Post-Quantum Cryptography impact in Life Sciences

Pharmaceutical research data (confidentiality)

Lab equipment firmware update integrity

Clinical trial subject data (privacy)

Clinical trial results (confidentiality and integrity)

Manufacturing data (IP, integrity and confidentiality)

Genomic data (confidentiality and integrity)

Access control (systems, privacy)

Quantum Safe Actions for Healthcare and Life Science Security

Migrate electronic health records (EHR), trial data, and genomic datasets to NIST-approved PQC algorithms to protect patient privacy and research integrity for decades.

Deploy PQC-ready HSMs and KMS in healthcare IT and biotech environments to secure sensitive patient identifiers, drug formulas, and clinical trial keys.

Secure connected medical devices, telehealth, and IoMT traffic with hybrid PQC protocols to prevent eavesdropping and data manipulation in patient care.

Mandate PQC compliance in contracts with CROs, medical device suppliers, and research collaborators to safeguard the extended healthcare and life sciences ecosystem.

Enable crypto-agility across clinical systems, medical devices, and cloud platforms so hospitals, labs, and pharma firms can rapidly switch to stronger protections as standards evolve.

Adopt quantum-safe digital signatures for electronic prescriptions, medical imaging systems, lab software, and regulator submissions to ensure authenticity and non-repudiation.

Maintain a live inventory and continuous monitoring of all cryptographic assets across EHR platforms, supply chain systems, and R&D applications.

Establish a quantum-safe governance and compliance roadmap aligned to HIPAA, GDPR, FDA, EMA, and other health data protection regulations.

Call to Action

Umut Cikla
IBM Quantum Safe Asia Pacific Leader
umut.cikla@ibm.com

Notices and disclaimers

This document is distributed “as is” without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM.

Not all offerings are available in every country in which IBM operates.

Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at: www.ibm.com/legal/copytrade.shtml.

Certain comments made in this presentation may be characterized as forward looking under the Private Securities Litigation Reform Act of 1995.

Forward-looking statements are based on the company’s current assumptions regarding future business and financial performance. Those statements by their nature address matters that are uncertain to different degrees and involve a number of factors that could cause actual results to differ materially. Additional information concerning these factors is contained in the Company’s filings with the SEC.
Copies are available from the SEC, from the IBM website, or from IBM Investor Relations.

Any forward-looking statement made during this presentation speaks only as of the date on which it is made. The company assumes no obligation to update or revise any forward-looking statements except as required by law; these charts and the associated remarks and comments are integrally related and are intended to be presented and understood together.