**Qryptonic Ideal Customer Profile (ICP) – Hospitals & Healthcare**

**1. Target Industry**

* **Primary Focus**: **Hospitals, Healthcare Systems, and Medical Research Institutions**
* **Secondary Focus**: **HealthTech Companies, Pharmaceutical Firms, and Insurance Providers**

**2. Key Decision Makers & Influencers**

🔹 **Chief Information Security Officer (CISO)** – Oversees security risk management & compliance.  
🔹 **Chief Information Officer (CIO)** – Manages IT infrastructure, security strategy, and tech investments.  
🔹 **Chief Compliance Officer (CCO)** – Ensures regulatory compliance (HIPAA, HITRUST, NIST).  
🔹 **VP/Director of IT Security** – Handles day-to-day security operations and implementations.  
🔹 **Chief Risk Officer (CRO)** – Focuses on enterprise risk management, including cyber threats.  
🔹 **Hospital Executives (COO, CEO, CFO)** – Prioritize business continuity, patient trust, and financial risk.

**3. Key Challenges Hospitals Face**

**🚨 Cybersecurity Risks in Healthcare**

* **Data Breaches & Ransomware Attacks** → Healthcare was the #1 target for ransomware in 2024. Attackers exploit vulnerabilities in **electronic health records (EHRs), IoT devices, and medical databases**.
* **Nation-State & APT Threats** → Healthcare data is **high-value for cybercriminals & espionage**, leading to state-backed threats.
* **Harvest Now, Decrypt Later (HNDL)** → Hackers are already **stealing encrypted patient data** to decrypt when quantum computing matures.

**🛑 Regulatory Compliance & Risk Management**

* **HIPAA & HITRUST Compliance** → Ensuring encrypted patient records remain secure under evolving **NIST post-quantum standards**.
* **Medical IoT Security** → MRI machines, infusion pumps, and patient monitoring systems rely on **outdated encryption methods** vulnerable to quantum attacks.
* **Third-Party & Supply Chain Risks** → Many hospitals depend on external software vendors with **unknown cryptographic risks**.

**⚠️ The Post-Quantum Threat**

* **RSA & ECC Encryption Won’t Hold** → Quantum computers will break RSA-based encryption, used in **EHRs, patient portals, and secure communications**.
* **Regulatory Pressure Is Mounting** → The White House’s **National Cybersecurity Strategy** mandates a shift to **post-quantum cryptography (PQC)**. Hospitals **must act now** to stay compliant.

**4. Why Qryptonic? – The Solution for Hospitals**

✅ **Quantum-Resilient Data Protection**

* **Post-Quantum Cryptography (PQC) Readiness Assessments** → Helps hospitals **evaluate encryption vulnerabilities** before quantum threats emerge.
* **NIST-Certified Quantum-Safe Encryption** → Deploys **CRYSTALS-Kyber & Dilithium** to safeguard **patient records, medical research, and payment systems**.

✅ **End-to-End Healthcare Cybersecurity**

* **Quantum Risk Simulator** → Identifies **vulnerable EHR systems, IoT devices, and medical applications** at risk from quantum decryption.
* **Crypto-Agility for Healthcare IT** → Enables hospitals to **seamlessly transition** to quantum-secure cryptographic standards.
* **Medical Device Security Compliance** → Protects **connected medical devices** from quantum attacks.

✅ **Regulatory Alignment & Compliance Support**

* **Meets NIST & HIPAA Encryption Standards** → Ensures compliance with **HITRUST, HHS, and upcoming federal mandates**.
* **Incident Response & Risk Mitigation** → Helps hospitals build a **crypto-agile security roadmap** that **aligns with federal guidelines**.

✅ **Protects Hospital Revenue & Reputation**

* **Reduces Risk of Lawsuits & Fines** → Non-compliance with encryption standards could lead to **hefty fines** and **lawsuits from data breaches**.
* **Safeguards Patient Trust** → Quantum-resistant security ensures **long-term patient data integrity**.

**5. Buying Triggers – When Hospitals Need Qryptonic**

🔹 **Regulatory Changes & Compliance Audits** – New NIST standards push for **post-quantum encryption mandates**.  
🔹 **Security Breach or Ransomware Attack** – Hospitals seeking **stronger encryption solutions** post-incident.  
🔹 **Medical IoT Expansion** – Increased use of **connected medical devices** requiring **quantum-safe security**.  
🔹 **EHR Upgrades & Migrations** – IT leaders looking to secure **patient data for the next decade**.  
🔹 **Cyber Insurance Mandates** – Insurers **requiring** quantum-safe encryption to reduce policy risks.

**6. How to Engage & Sell to Hospitals**

🔹 **Lead with Risk Awareness** – Position quantum security as a **must-have compliance & patient safety measure**, not just an IT upgrade.  
🔹 **Align with Compliance Needs** – Highlight how Qryptonic ensures hospitals **meet HIPAA, HITRUST, and federal security mandates**.  
🔹 **Showcase ROI & Risk Reduction** – Help decision-makers see that **proactive security prevents costly breaches, lawsuits, and operational downtime**.  
🔹 **Offer a Post-Quantum Risk Assessment** – Hospitals need **visibility into encryption vulnerabilities**—make this the entry point.

**7. Next Steps – Call to Action**

📢 **Hospitals: Don’t Wait for a Crisis to Secure Your Data**  
**Contact Qryptonic today for a Post-Quantum Readiness Assessment.**

**🔹 Website:** [www.qryptonic.com](http://www.qryptonic.com)  
**📩 Email:** info@qryptonic.com

🚀 **Future-proof your hospital’s cybersecurity—before it’s too late.**