

SECURING THE FUTURE OF HEALTHCARE THROUGH QUANTUM PROTECTION

Prepared by Quantum Kancil Durian (QKD)



Teh Zhi Jian



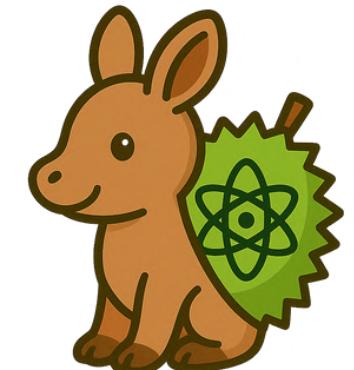
Tiong Yong Qing



Choo Tze Yee



Pah Onn Qi



A detailed 3D rendering of a quantum computing system. It features several concentric rings of blue and gold-colored components, likely superconducting qubits or readout electronics, arranged in a cylindrical shape. Numerous thin, glowing yellow lines represent data lines or control signals connecting the different parts. The overall design is intricate and futuristic.

Background

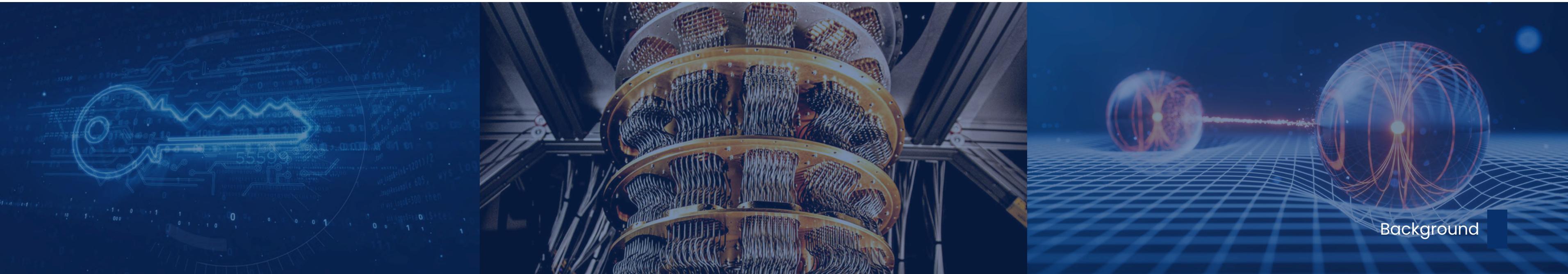
Introduction

Quantum Technology

harnesses the principles of quantum physics, such as **superposition** and **entanglement** to enable breakthroughs like ultra-powerful computing and highly secure communication.

Quantum Cryptography

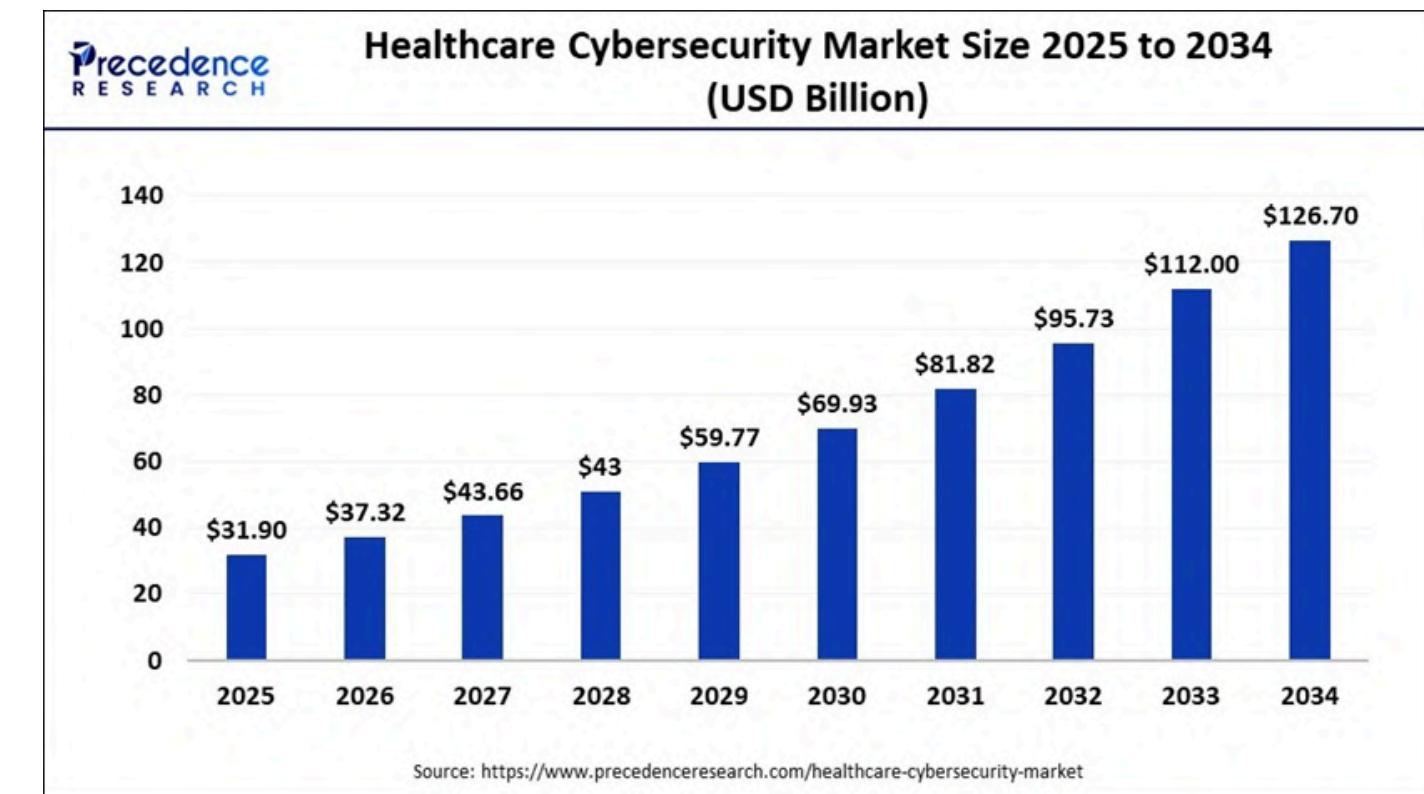
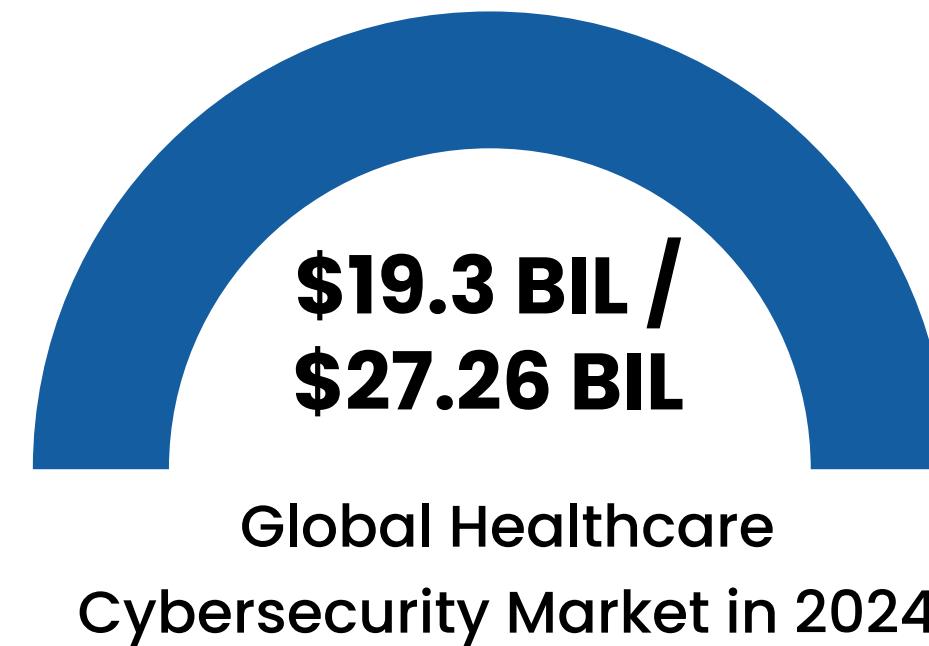
applies these principles to **information security**, enabling encryption that is inherently resistant to hacking since any interception attempt is immediately detectable.



Background

Healthcare Cybersecurity Market Landscape

The **rapidly growing** cybersecurity market, driven by **rising threats** and the **shortcomings** of **classical encryption**, is fueling urgent demand for stronger, future-proof solutions, positioning **quantum encryption** as an **attractive investment**.



The global healthcare cybersecurity market is expected to experience substantial growth. One forecast predicts it will reach **USD 75.04 billion by 2032**, with an **18.8% Compound Annual Growth Rate (CAGR)**. Another projection sees the market expanding to **USD 126.70 billion by 2034**, with a **16.61% CAGR**.

Source: [Fortune Business Insights. Healthcare Cybersecurity Market](#). (Accessed 8 Sep 2025);
: [Precedence Research. Healthcare Cybersecurity Market Size, Share, and Trends](#). (Accessed 8 Sep 2025)

Background

Healthcare Cybersecurity Market Landscape



North America

held the **largest market share in 2024**, accounting for **(39.07% of the global market)**.



Asia-Pacific

is anticipated to experience **strong growth of 20%** due to rising awareness, increased cyberattacks, and the adoption of advanced cybersecurity solutions.

Healthcare Cybersecurity Market Landscape

Key Growth Drivers



The market is being fueled by an **increase in cyberattacks** and **rising privacy concerns**.

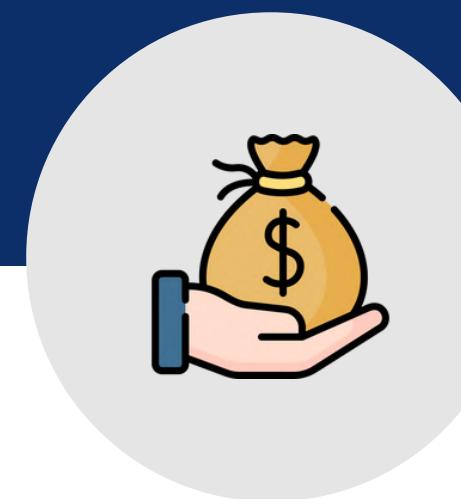


Growth is also **driven** by the **widespread adoption** of **new technologies** such as the Internet of Things (IoT), 5G, and cloud computing.



Increased regulatory requirements and the growing number of connected medical devices are also **major factors**.

Rising Threats and Industry Vulnerabilities



High Value Target

Medical identities are a **prime target** for **cybercriminals**.



Malaysia's Exposure

Malaysia ranks **11th** globally in **data breaches** and **leakage**



Critical Sensitivity

Breached medical data includes **personal, genetic, and clinical information**

Rising Threats and Industry Vulnerabilities



Ongoing Threat

Malaysia views **data leakage** as a **growing** and **serious** cybersecurity **threat**.



Future Risk

With "**Harvest Now, Decrypt Later**", classical cryptography is **no longer sufficient**.



Problem statement

Problem Statement



Classical encryption methods face inherent technical limitations.

Healthcare systems are vulnerable to frequent cybersecurity breaches.

These incidents compromise patient privacy, cause business losses, and disrupt critical operations.



Technology Limitations in Classical Encryption

Background

1

Classical encryption (RSA, ECC, DH) depends on problems like **integer factorization** and **discrete logarithms**. While secure against today's computers, these foundations will **collapse once quantum computers become practical**.

2

Sensitive data has a **long shelf life** like government secrets, medical records, intellectual property, and defense information remain valuable for decades. These data can be **stolen now** and stored until it can be **decrypted in the future**, making the quantum threat invisible but very real.

Technology Limitations in Classical Encryption

Insufficient Encryption

1

“Harvest Now, Decrypt Later” (HNDL) attacks pose a growing risk. With quantum Shor’s algorithm, quantum computers could **break classical encryption in hours**, turning the strongest digital locks into open doors. It’s not a question of if this will happen, but when.

2

The cost of data storage is **minimal**, meaning adversaries can easily accumulate vast amounts of encrypted information today and patiently wait for the tools to **unlock it tomorrow**.

3

Classical cryptography is **reaching its limits**, and with the rise of quantum computing, it will soon be obsolete.

Cybersecurity Breaches in Healthcare

Electronic medical records are now widely adopted, with increasing reliance on online healthcare portals to manage and protect patient data. However, this growing digitalization has also led to a rise in cybersecurity breaches.



Personal medical records are valued at **20-50 times** more than financial identities.



have their patient medical records leaked.

This highlights a widespread, systemic vulnerability in healthcare data security. It could take place in any health facility, including private hospital services and medical centres at higher institutions of learning.



Cybersecurity Breaches in Healthcare



Malaysia ranks **11th** in the **most breached countries** in the world.

1

Data of nearly **20,000 Malaysian patients** are exposed online (names, birthdates, and examination dates).

2

About **1.2 million** sensitive medical images (**x-rays, CT, MRI scans**) were leaked.

3

Malaysia's Ministry of Health is addressing this issue with urgency, given the risks of patient data exposure.

4

"The threat to cybersecurity is continuous and requires much more skills and expert manpower to tackle it" – Health Minister Dzulkefly Ahmad

Business Loses and Disruptions

Cyberattacks on hospitals often cause **severe operational disruptions** and **significant financial losses**. For instance, a cyberattack on a Southern California healthcare provider affected three hospitals, stealing **17 million patient records** and **forcing a return to paper processes**, which disrupted operations for both patients and staff.

213 DAYS

Average time to identify a cyberattack in the healthcare sector and an **additional 83 days** to contain it.

\$9.77 MIL

Average cost of a healthcare data breach, **67% higher** than the **global average of \$4.88 million** – the highest among 17 industries studied.

\$700,000

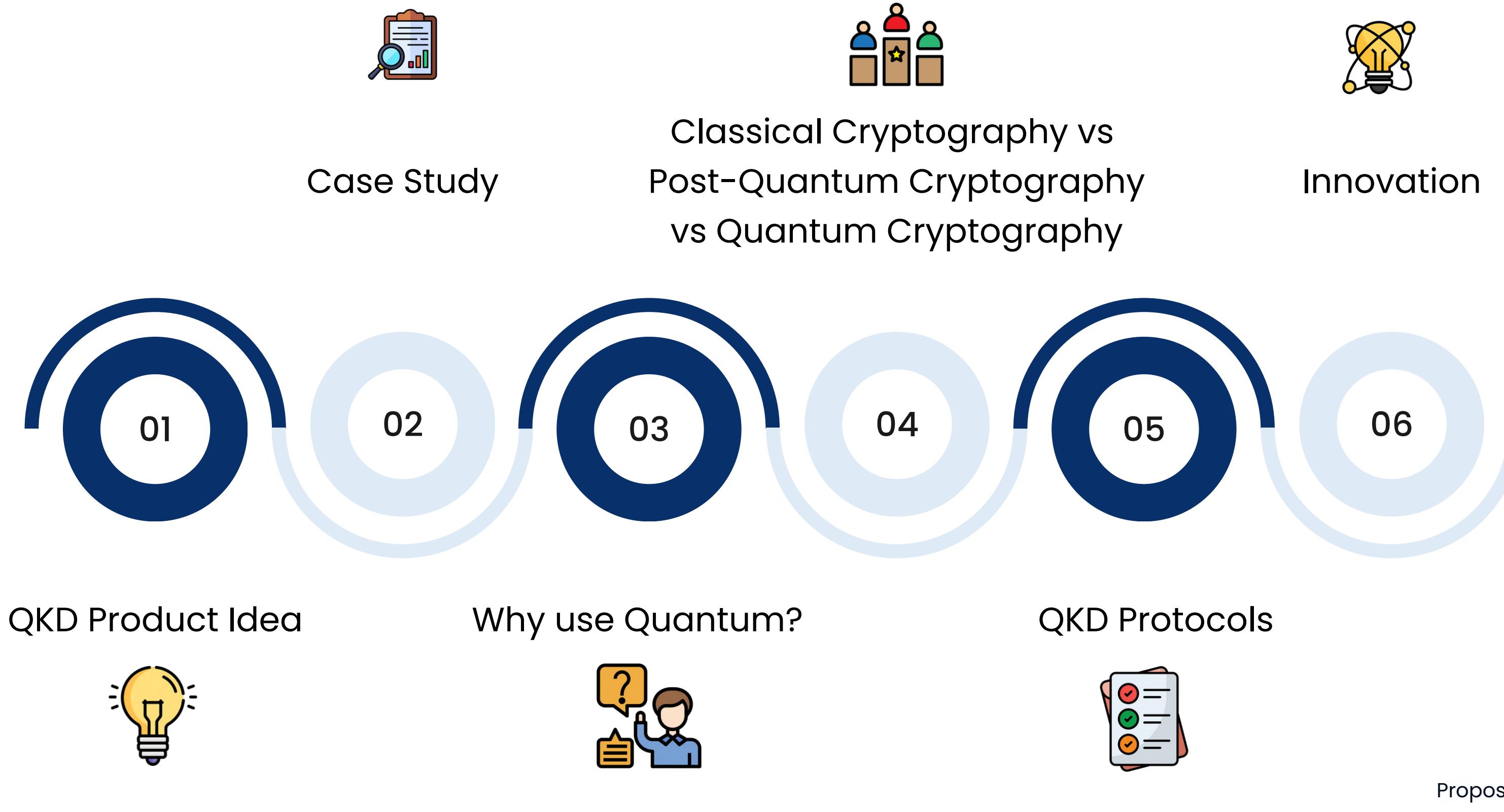
Average costs include expenses for forensics, data recovery, crisis management, and business interruption.

Source: [Bank Info Security. Hackers Steal 17M Patient Records in Attack on 3 Hospitals](#) (Accessed 8 Sep 2025);
: [GHP News. The Average Cost of a Data Breach in the Healthcare Sector](#) (Accessed 8 Sep 2025);
: [CHUBB. Cyber insurance for the healthcare industry](#) (Accessed 8 Sep 2025)



Proposed Solutions

Proposed Solution Flow



QKD Product Idea

Here we propose a **Quantum-enabled framework** that overcomes the limitations of classical encryption and strengthens healthcare data transfer. By integrating Quantum Key Distribution (QKD), our framework **protects both the transfer pipeline and patient portal interactions** by enabling:

Secure Quantum-Assured Transfers

Medical records are encrypted and exchanged with QKD-derived keys, ensuring confidentiality across provider networks.

Staff and Patient Portal Access

Retrieved records are re-encrypted with QKD-backed session keys prior to delivery, achieving true end-to-end protection.



QKD Product Idea



OBJECTIVE:

To deliver a **scalable quantum-security framework** that empowers healthcare providers to streamline secure record transfers while safeguarding patient confidentiality.

Case Study: Pre-existing Company on Quantum Solutions



ID Quantique (IDQ)

- **IDQ** is an company that offers carrier-grade **QKD systems** for governments, telecoms, and financial institutions.
- **Healthcare Use Case (Austria):**
 - **Objective:** Securely share sensitive data between Medical University Graz and Landeskrankenhaus Graz II.
 - **Data Transferred:** High-volume data, including digital histological slides (10GB per image), as well as clinical and genetic data.
 - **Technology Stack:**
 - **QKD:** Provides a secure foundation for data transmission.
 - **fragmentix CLUSTER:** Further enhances security through data fragmentation and secret sharing.



China's Quantum Network (USTC / China Telecom)

China has a strong incentive to build a quantum network due to its ability to provide secure, long-distance communication. The country has made significant progress in this area, demonstrated by two major projects:

- **Beijing–Shanghai QKD Backbone (2,000 km):** Secure quantum key distribution across major cities using fiber and relay nodes for continuous, high-security communication.
- **Satellite-Enabled QKD (Global Reach):** The Jinan-1 microsatellite enabled secure quantum key exchange over 12,900 km, connecting China with South Africa.

Source: [ID Quantique. Fragmentix quantum-safe storage solution \(2020\);](#)

[: University of Science and Technology of China. Beijing–Shanghai Quantum Communication Network Put into Use \(2017\);](#)

[: University of Science and Technology of China. USTC Develops Quantum Microsatellite and Achieves Real-Time QKD Between Microsatellite and Mobile Ground Stations \(2025\).](#)

Proposed Solutions

Case Study: Pre-existing Company on Quantum Solutions



Quantum Computing Inc. (QUBT)

QUBT is a company that provides **quantum communication** and **cybersecurity solutions**.

- **Cybersecurity use case:** Delivered quantum-safe communication to a Top 5 US bank to secure sensitive transactions and client data.



Toshiba

Toshiba's recent quantum projects include:

- Deploying QKD networks for financial institutions in Japan and the UK.
- Partnered with BT and EY in April 2022 to launch the first commercial trial of a quantum-secured metro network in London.

Source: [Quantum Computing Inc. Secures Purchase Order from Top 5 U.S. Bank to Advance Quantum Cybersecurity Testbed](#). (Accessed 8 Sep 2025);

: [Toshiba, BT and Toshiba to build world's first quantum-secured commercial metro network across London](#). (Accessed 8 Sep 2025)

: [EY, BT and Toshiba launch first commercial trial of quantum secured communication services – EY becomes first commercial customer](#). (Accessed 8 Sep 2025)

Proposed Solutions

Why use Quantum: Technology Perspective?



Future-Proof Security:

Based on quantum physics, not just mathematical hardness — immune to quantum computer attacks.



Physical-Layer Protection:

Guarantees security through the laws of nature (no-cloning or measurement disturbance).



Zero Leakage Assurance:

Even if data is intercepted, it's useless because it can't be decrypted without the correct quantum key.

Why use Quantum: Technology Perspective?



Long-Term Confidentiality:

Crucial for sectors like healthcare, government, defense, and intellectual property.



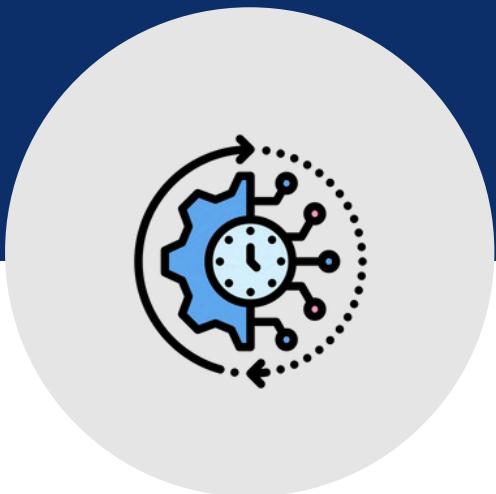
Compliance & Regulation:

Quantum technology supports strict data protection standards, such as PDPA, HIPAA, and GDPR.



Trust & Reputation:

Commitment to protecting patients, customers, and regulators with future-proof security.



Future Readiness:

Ensuring resilience against next-generation threats.

Why use Quantum: Industry Perspective?

1

2

Massive Government Investments

- The UK has committed **£670 million** to quantum technologies, with the goal of building a national quantum network and quantum internet by **2035**.
- Similar large-scale funding from the US, EU, China, and Singapore, **signaling global momentum.**

Proven Real-World Trials

- UK's NHS pilot projects **successfully tested quantum-safe patient data transfers**, protecting critical healthcare infrastructure.
- **Telecoms** and **financial institutions** are testing QKD for **secure communication**.

Why use Quantum: Industry Perspective?

3

Quantum Advantage by 2035

- **Forecasts** show accessible quantum computers capable of **1 trillion operations**, delivering benefits **beyond classical supercomputers**.
- Industries expect **breakthroughs** in finance, healthcare, energy, defense, and supply chain security.

4

Competitive Edge & Funding Attraction

- Companies are **incentivized** to **adopt quantum technologies** early as it can **attract** government grants, investor confidence, and strategic partnerships.
- Being **“quantum-ready”** signals innovation leadership, securing stronger positions in global markets.

Classical vs PQC vs Quantum Cryptography

| | Classical Cryptography | Post-Quantum Cryptography (PQC) | Quantum Cryptography |
|-------------------------------|---|--|---|
| Devices | Classical computers | Classical computers | Quantum devices (or hybrid with classical) |
| Security relies on | Problems like integer factorization, discrete logarithm | Hard problems believed to resist quantum attacks (lattices, codes, etc.) | Quantum mechanics (laws of physics) |
| Threat from quantum computers | Broken by Quantum Algorithms: Shor's algorithm and Grover's algorithm | Designed to resist quantum attacks | Naturally resistant since security is physical |
| Examples | RSA, Diffie-Hellman, ECC | Kyber, Dilithium | QKD (BB84 protocol) |
| Key idea | Math hardness for classical computers | Math hardness resistant to both classical & quantum computers | Physics of quantum states (no-cloning theorem, measurement disturbance) |

Classical vs PQC vs Quantum Cryptography

Classical Cryptography

- Classical methods (RSA, ECC, DH) depend on problems like **factorization and discrete logs**.
- With the arrival of quantum computers, these problems **can be solved in hours** instead of billions of years, **leaving classical encryption defenseless**.



PQC

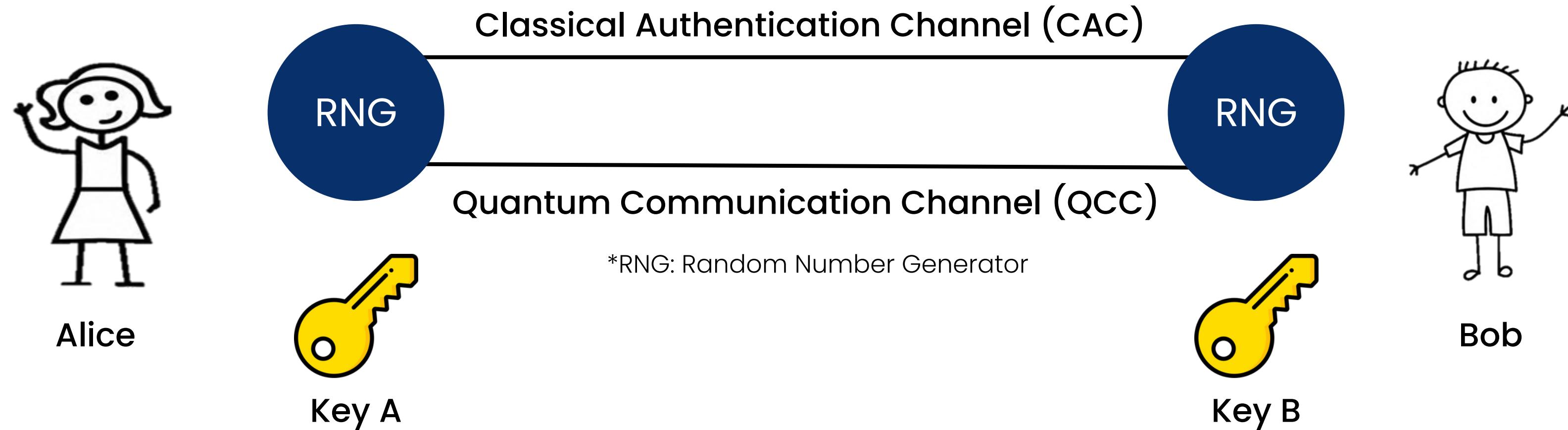
- PQC **depends on assumptions about problem hardness**, with no guarantee they will hold against future quantum advances.
- A **future breakthrough in mathematics or algorithms could collapse PQC**, just as Shor's algorithm broke RSA and ECC.
- PQC buys us time, but **does not guarantee long-term security**.

Quantum Cryptography

- Not math-based – physics-based: **Security relies on the laws of quantum mechanics**.
- Quantum Key Distribution (QKD):
 - Any eavesdropper must disturb the quantum state.
 - However, disturbance is detectable instantly.

- **Unbreakable by design:** Security is guaranteed by nature itself, not just computational hardness.

What is Quantum Key Distribution (QKD)?



Distribution Phase & Quantum Transmission Phase

Medical records are encrypted and exchanged with QKD-derived keys, ensuring confidentiality across provider networks.

Classical Transmission Phase

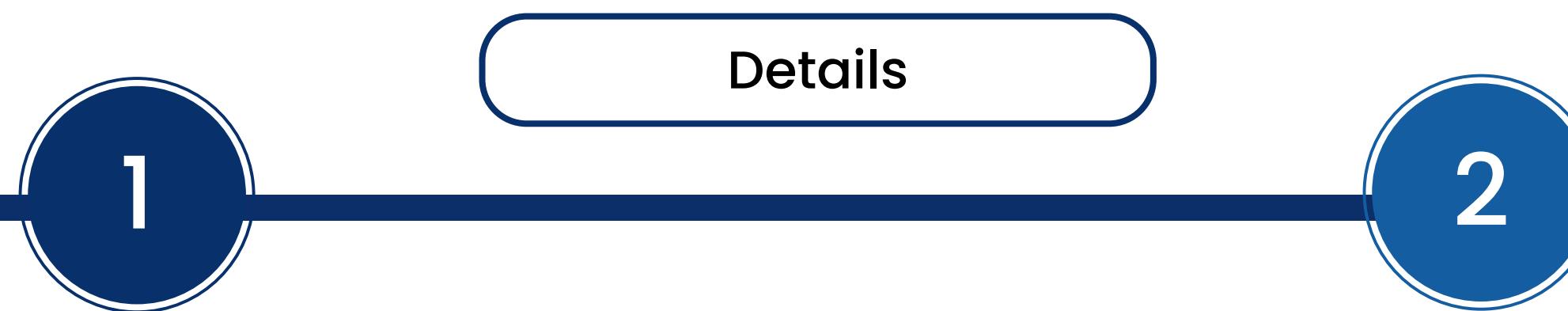
A process where sender A and recipient B communicate in a classical way, such as by exchanging information in the CAC.

Existing QKD Protocols: BB84 Protocol

In 1984, BB84 protocol was implemented by Bennett and Brassard as a first QKD scheme together with the paper that introduced quantum cryptography.

$$X = \begin{cases} 0, & \text{represent } |0\rangle \text{ in standard basis, } |+\rangle \text{ in Hadamard basis} \\ 1, & \text{represent } |1\rangle \text{ in standard basis, } |-\rangle \text{ in Hadamard basis} \end{cases}$$

$$\theta = \begin{cases} 0, & \text{Measurement in standard basis} \\ 1, & \text{Measurement in Hadamard basis} \end{cases}$$



Used to generate and measure single qubit quantum states, which is known as key in producing a shared key.

Used to transmit a key with length equal to the length of messages that ensure security unconditionally using the quantum properties like superposition, entanglement and uncertainty.

Existing QKD Protocols: Six-State Protocol

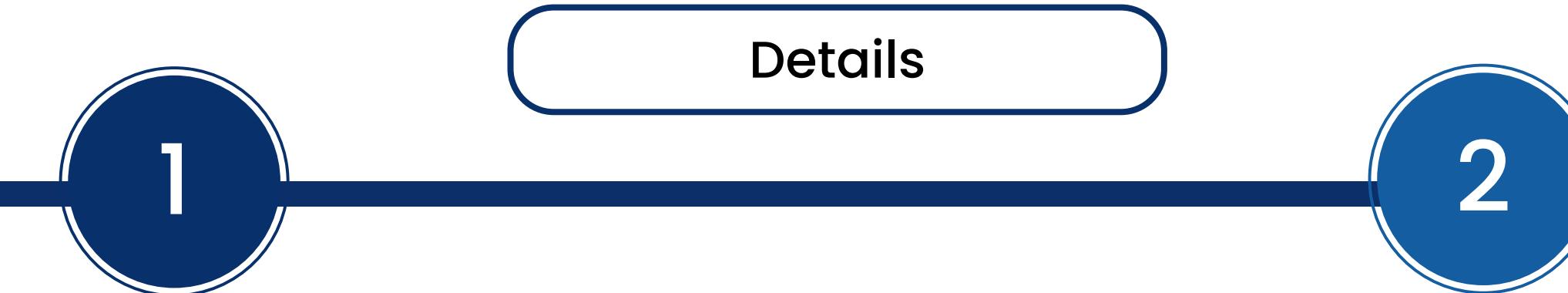
Vary based on the BB84 protocol and are robust to intercept-resend attack.

$$\sigma_z = \{|0\rangle, |1\rangle\}$$

$$\sigma_x = \{|+\rangle, |-\rangle\}$$

$$\sigma_u = \left\{ |+y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |-y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \right\}$$

Details



More symmetrical than the standard BB84 protocol.

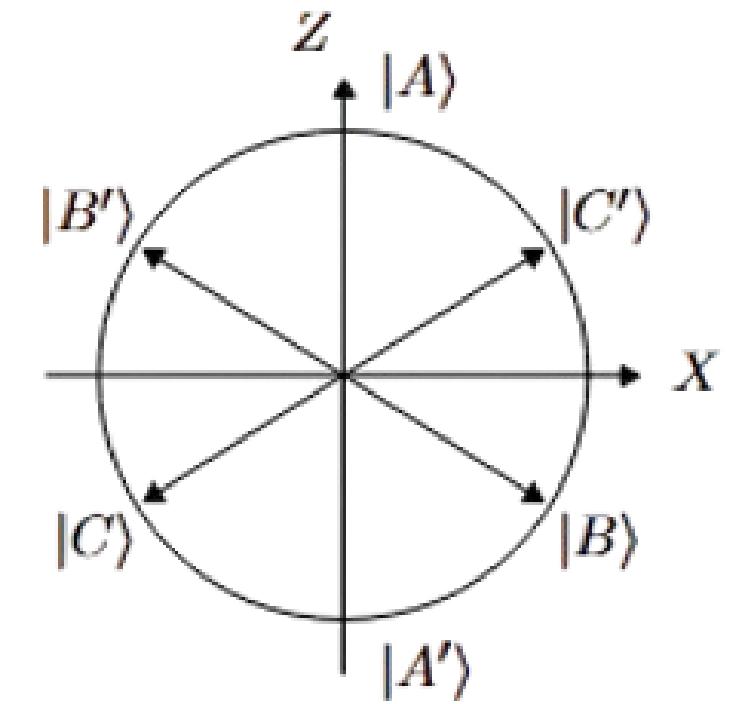
Useful when the collective-rotation noise is dominant in the communication channel and is designed to be robust against intercept-resend attacks.

Our Innovation: The Six-State Symmetric Protocol

6 quantum states separately into 2 detection sets.

$$\mathcal{S}_0 = \begin{cases} |A\rangle, & |0\rangle \\ |B\rangle, & \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle \\ |C\rangle, & -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle \end{cases}$$

$$\mathcal{S}_1 = \begin{cases} |A'\rangle, & |1\rangle \\ |B'\rangle, & \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle \\ |C'\rangle, & \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle \end{cases}$$



Details

1

2

Why it is known as Symmetric?

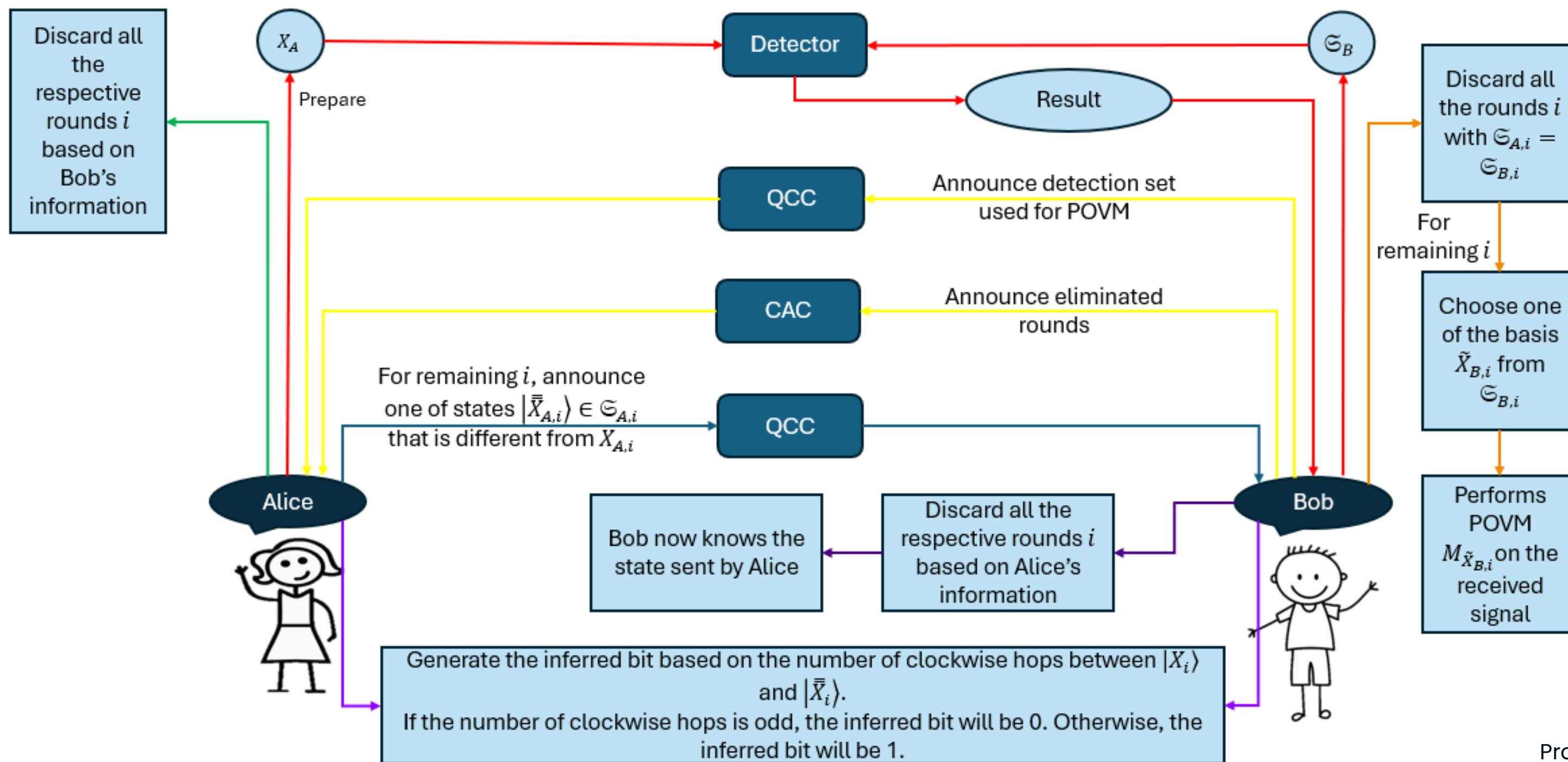
Uses the 6 states that are symmetric within their neighbouring quantum states with 60 degree.

Differences from Six-State Protocol:

Alice and Bob will not exchange the basis in the CAC but only the rounds information to decrease the amount of communication to ensure eavesdropper gets limited information in the CAC.

Our Innovation: The Six-State Symmetric Protocol

To **prepare n-bit string**, Alice needs to prepare $N=(6+\eta)n$ -bit string for $\eta \approx 0 \leq 1$ by choosing one quantum state from the two detection sets (X_A).



Comparison between Protocols

| | BB84 Protocol | Six-State Protocol | Six-State Symmetric Protocol |
|------------------|--|--|---|
| Number of State: |  |  |  |
| Correctness: | 100% | 100% | 100% |
| Security: | Probability to get information by Eavesdropper: $< 3/4 - \cos^2(\pi/8)$ | Abort the protocol if the error rate $> 1/3$, since this indicates the presence of eavesdropper attempt to perform intercept-resend attacks | 71.43% confidence with intercept-resend attacks |

Product Summary & Highlight

Quantum-Ready Framework:

This framework utilizes Quantum Key Distribution (QKD) for medical records encryption. By leveraging QKD, the encryption is **fundamentally unbreakable**.



It includes a **web application** with dedicated portals for both staff and patients.



Our solution is targeted at **private and government healthcare provider systems**.



Product Summary & Highlight

Our **quantum-enabled** framework secures healthcare data beyond classical encryption. It **protects transfers** and **patient portals** from end-to-end, with **Tracking and Data Watermarking** adding full lifecycle visibility to ensure accountability and leakage prevention.

1

Secure Quantum-Assured Transfers:

Medical records are **encrypted** with **QKD-generated keys**, keeping data confidential across healthcare provider networks.

2

Staff and Patient Portal Access:

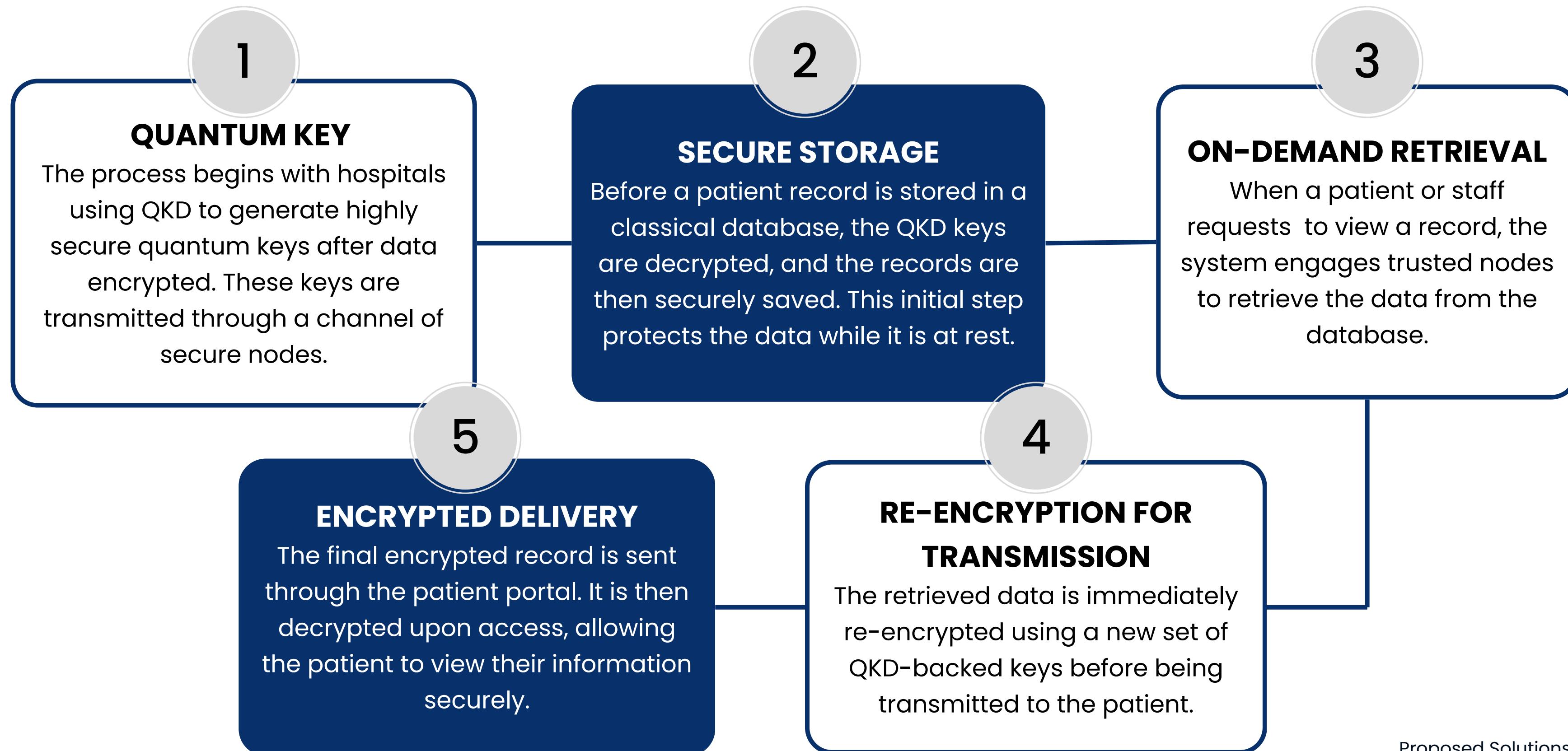
When patients access records, data is re-encrypted with fresh QKD session keys, guaranteeing true **end-to-end protection** from database to device.

3

Tracing with Data Watermarking:

To **stop unauthorized sharing**, we **embed unique watermarks** in every document, making it possible to trace the source of any leak.

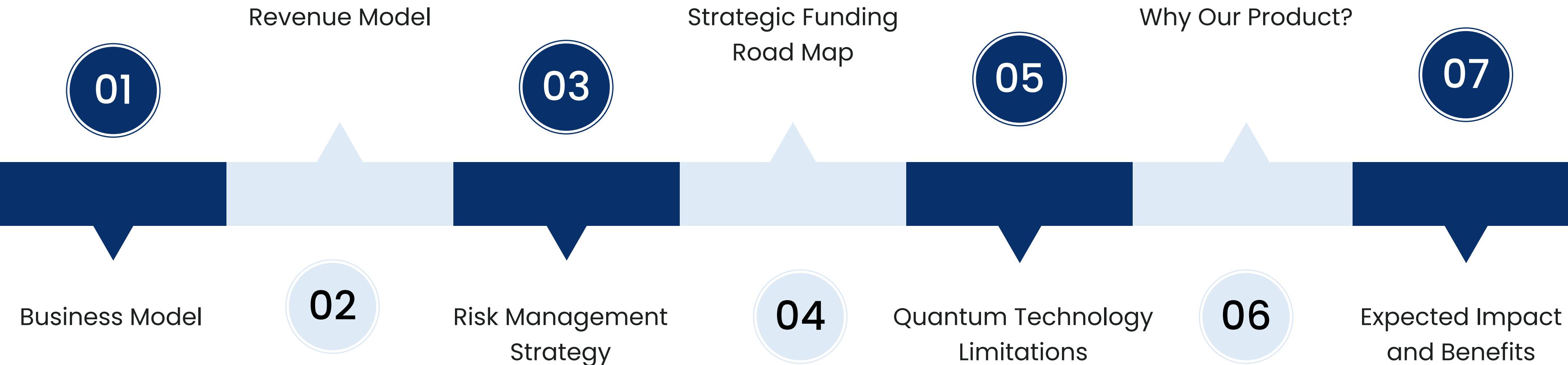
Product Summary & Highlight





Business Model & Roadmap

Business Model & Roadmap



Business Model

Our product is designed to serve a diverse range of healthcare providers, from large-scale government systems to individual private clinics.

Government Healthcare Systems

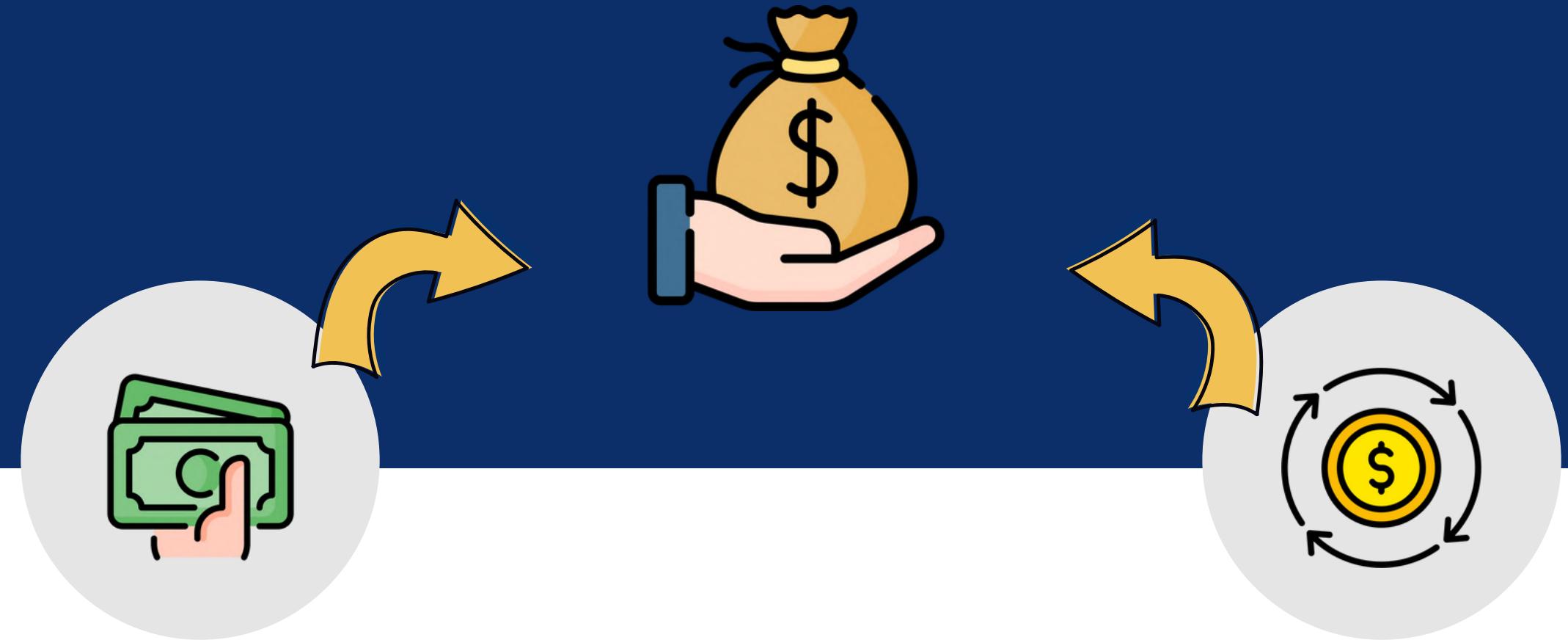
- Managed by federal, state, or regional bodies
- Includes public hospitals and clinics
- Serves the general population

Private Healthcare Providers

- **Private Clinics:** Small, independent practices and specialized clinics.
- **Small Private Hospitals:** Mid-sized hospitals that offer a range of services but operate on a smaller scale than major medical centers.
- **Large Private Hospitals:** Major medical centers, often part of hospital networks, that provide comprehensive, multi-specialty care.

Our product aims charge for the use of our quantum-secure infrastructure and framework, not for the volume of data transferred. As a result, the costs associated with your trusted nodes are not included in our service.

Revenue Model



One-time Project Fee

A **large, upfront payment** derived from government funding to cover the initial design, deployment, and integration of the QKD system.

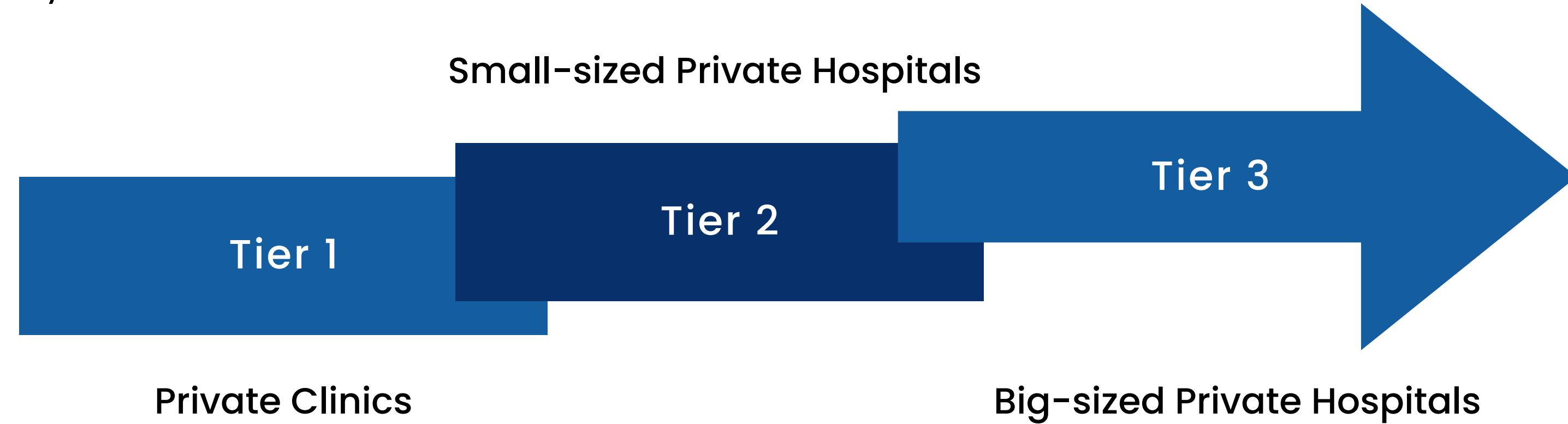
Recurring Subscription Plan

A **dedicated subscription plan** tailored exclusively for government clients, providing ongoing service, maintenance, and support for the established secure network.

Revenue Model: Private Healthcare Systems

Tiered Pricing Approach:

Designed to align with the scale and needs of different private healthcare providers. Our tiered structure is determined by the trusted node bandwidth and the volume of data transactions.



Revenue Model: Private Healthcare Systems

Tier 1: Private Clinics

A simplified, low-entry-point, flat-rate monthly or annual subscription fee.

This model avoids usage-based billing and covers a specific, limited number of secure connections, making it easy for small clinics to budget.



Revenue Model: Private Healthcare Systems



Tier 2: Small-sized Private Hospitals

Fixed base subscription for the core service and a variable fee based on amount of trusted nodes used.

This approach gives hospitals predictable costs for our secure framework, with the flexibility to scale fees during high-volume data transmissions.

Revenue Model: Private Healthcare Systems

Tier 3: Big-sized Private Hospitals

For our high-value enterprise solution, offer a dedicated, wide-spanning QKD network with a one-time installation and integration fee along with variable fee based on amount of trusted nodes used.

The recurring service subscription fee includes:

- **Variable fee component:** The service subscription fee includes a variable fee.
- **Unique Configurations:** This fee accounts for unique trusted node configurations.
- **High-Bandwidth Demands:** It covers the high-bandwidth demands of the network.
- **Significant Data Volume:** The fee also addresses the significant volume of data transactions.



Risk Management Strategy

1

Containment and Recovery Protocol

4

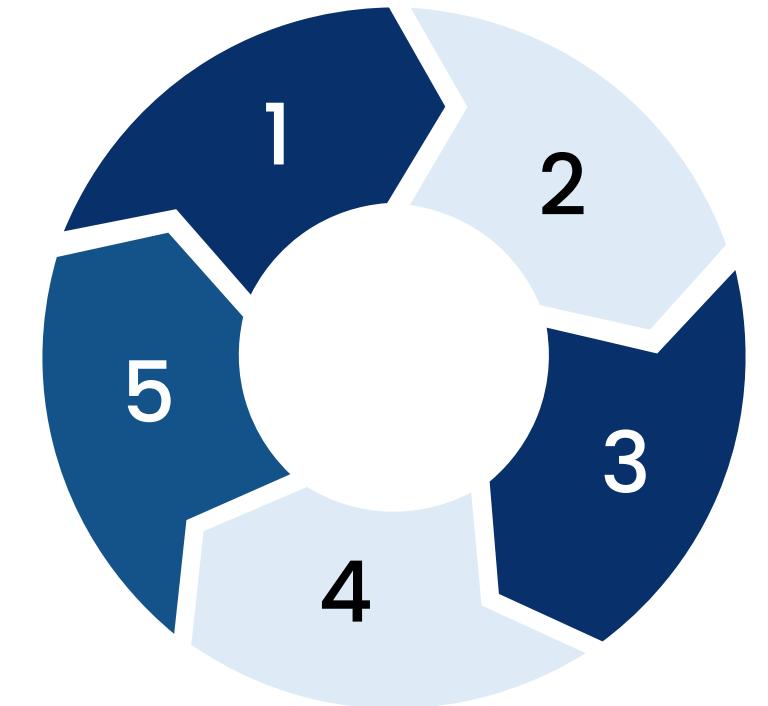
Isolate Compromised Systems:

Immediately disconnect affected systems from the network to prevent the breach from spreading. This could mean taking servers offline, revoking access to cloud services, or blocking specific IP addresses.

2

Preserve Digital Evidence:

Lock down all log files and system data. This action is essential for the forensic investigation and any future legal action.



Rebuild and Restore from Secure Backups:

If systems were corrupted, restore them from a known-clean backup. Ensure that the backup itself was not compromised.

3

Routine IT Maintenance and Upgrades:

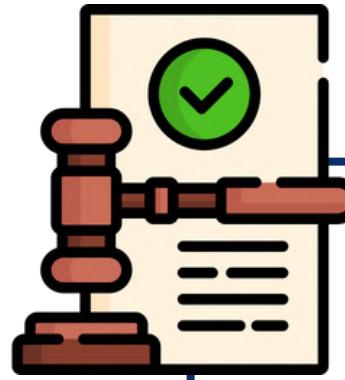
Invest in routine IT maintenance and security upgrades as a non-negotiable business expense to prevent future incidents.

5

Revise Your Incident Response Plan:

Conduct a post-incident analysis to identify procedural gaps and vulnerabilities. This review will inform a revised incident response framework, making it more efficient and robust for future threats.

Risk Management Strategy: Legal Compliance



1

Legal Counsel Fees:

Immediately engaging a lawyer specializing in data privacy is a top priority. They guide your response to ensure compliance with all applicable laws (like the GDPR, CCPA, or Malaysia's PDPA) and help manage potential liabilities.



2

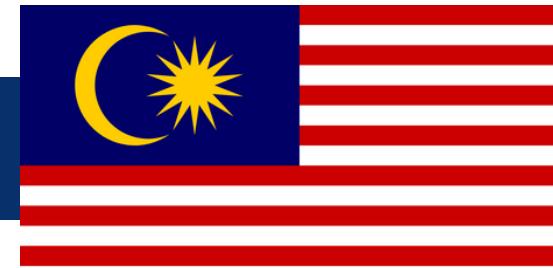
Breach Notification Costs:

For immediate legal compliance, we must take action to notify all affected individuals and regulators, covering the costs for communication channels and a dedicated call center. Additionally, we are required to secure and fund mandatory credit monitoring services for all impacted parties as required by law.

Risk Management Strategy: Legal Compliance

3

Regulatory Fines and Penalties



The **Personal Data Protection (Amendment) Act 2024** imposes stricter penalties, including fines of up to RM1 million and imprisonment of up to three years for breaches, with mandatory data breach notification carrying penalties of up to RM250,000 and two years' jail.

The **California Consumer Privacy Act (CCPA)** enforces civil penalties of up to \$2,500 per unintentional violation and \$7,500 per intentional violation, with each affected consumer's data counted separately, making large-scale breaches potentially costing millions.

In Singapore, the **Personal Data Protection Commission (PDPC)** can impose penalties of up to SGD 1 million or 10% of an organization's annual turnover, whichever is higher, for data protection breaches.

Source: [HHQ. New Data Breach Notification Requirements under the Personal Data Protection \(Amendment\) Act 2024.](#) (Accessed 8 Sep 2025)

: [Palo Alto Networks. What Is the California Consumer Privacy Act \(CCPA\).](#) (Accessed 8 Sep 2025)

: [Roedl. Updates on Personal Data Protection.](#) (Accessed 8 Sep 2025)

Business Model & Roadmap

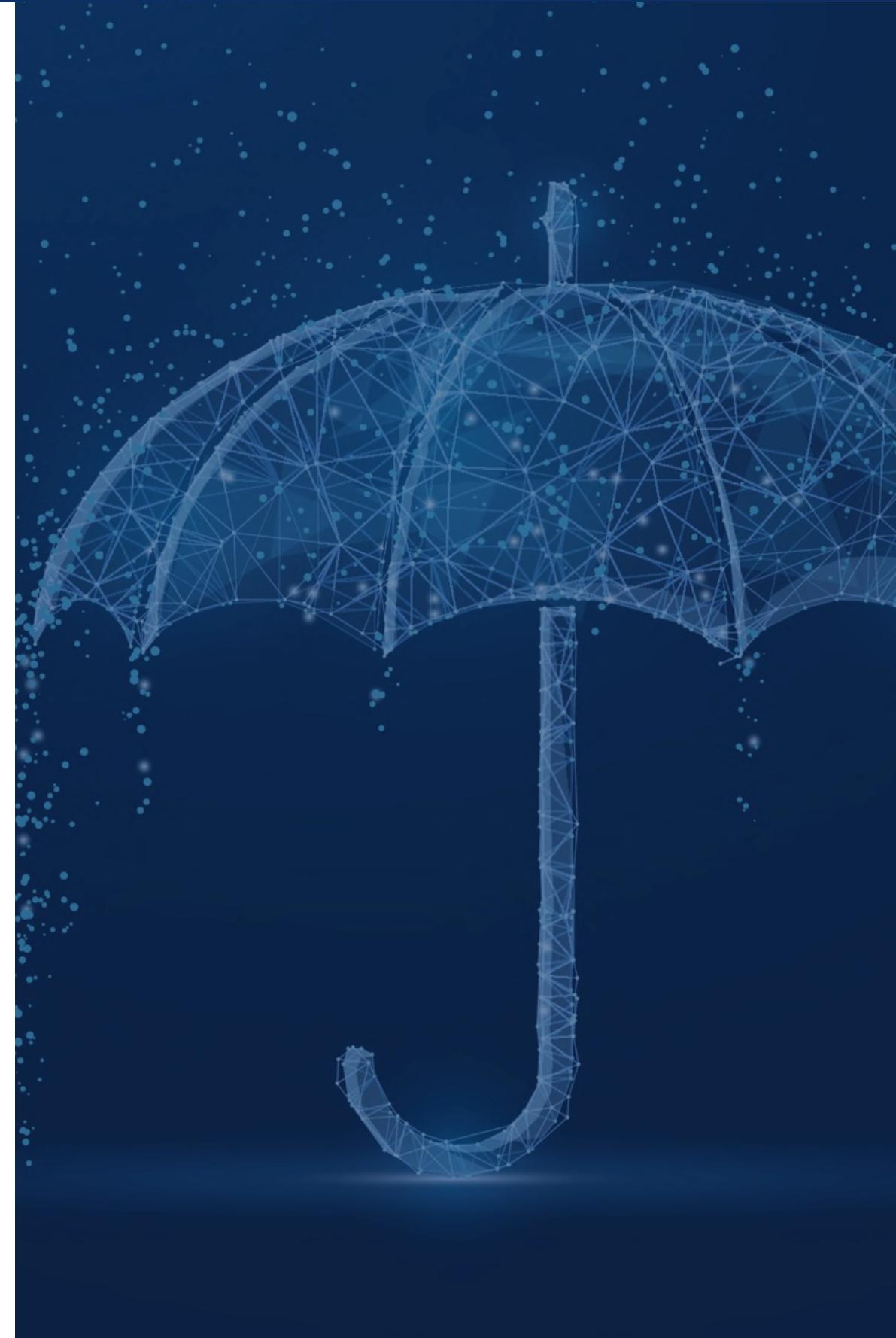
Risk Management Strategy

Over the counter cyber protect insurance

Cyber insurance protects businesses from data breaches, covering a company's own losses and legal costs from others. It covers both first-party costs your company directly faces, like business interruption and data restoration, and third-party liabilities, such as legal fees and fines from regulators.

Quantum computing could **reduce data leakage risks**, making some cyber insurance coverage **less critical**, especially for **third-party liabilities** and **hacker theft**.

As a result, quantum technology could lead to **lower cyber insurance premiums** due to a decrease in breach-related costs.



Strategic Funding Road Map

This timeline aims to outline our phased funding strategy, beginning with government grants to de-risk early development and progressing toward venture capital investment to enable significant scaling.

1

Phase 1: Government Funding &
Proof of Concept



2

Phase 2: Private Revenue and
Venture Capital



Phase 1: Government Funding & Proof of Concept

Our initial focus is on **leveraging government grants** to build our foundational technology and a compelling proof of concept. This approach allows us to demonstrate our product's viability without giving up early equity. We will target the following grants:



- Malaysia Digital Acceleration Grant
- Malaysia Digital X-Port Grant



- National Technology & Innovation Sandbox



- Ministry of Science, Technology, and Innovation (MOSTI) Grant Programs (TeD, BGF, SRF)

Upon securing these grants, we will build a robust infrastructure and a tangible product that proves our concept and its value.

Phase 2: Private Revenue and Venture Capital

Once our proof of concept is established and the initial infrastructure is built, we will transition to securing private funding. This phase will involve two key actions:

1

Establishing a Private Revenue Model

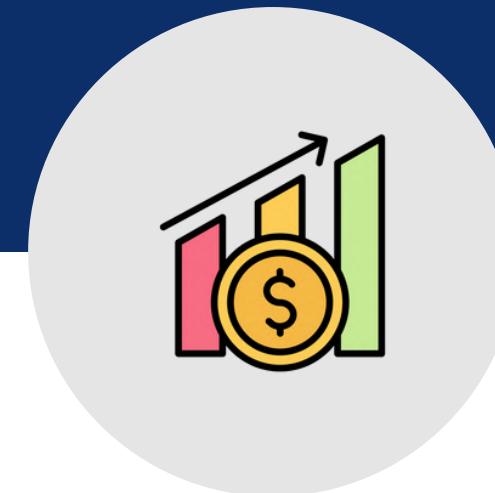
We will implement a clear and viable revenue model to show financial sustainability and market traction.

2

Approaching Venture Capital

With a proven product and a revenue-generating model, we will approach venture capitalists. This data-driven pitch will position us as a low-risk, high-growth opportunity, making us an attractive investment for scaling our enterprise and capitalizing on the quantum technology market.

Quantum Technology Limitations



Limited Range and Infrastructure

- QKD currently has a **restricted range**, even with "trusted nodes" that are **not truly quantum**.
- A fully quantum, long-distance network is a future goal, with the "**Quantum Internet**" and space-based QKD networks still in early development.
- Infrastructure for long-range QKD is progressing and will be **ready in the future**.

Immature and Costly Hardware

- There is **no commercial Quantum hardware** yet, as development is still in its **early stages**. Current systems run on **1,121 superconducting qubits**, yielding only **28 logical qubits, insufficient** for large-scale applications.
- These systems are **not yet fault-tolerant** and still **prone to errors**, leaving them **unsuitable** for widespread, large-scale deployment.
- The **dependence on specialized, costly equipment** and complex error-correction highlights both the **immaturity** and **high expense** of current technology.

Why Our Product ?

1

The Quantum Leap, Seizing a Future-Forward Market:

Despite current technological limitations, our product demonstrates strong potential, driven by:

- **Future-Ready Alignment** – Built to match the industry's strong shift toward quantum technology.
- **Backed by Momentum** – Reinforced by heavy investment from governments and private firms, signaling clear market growth.
- **Leakage Prevention** – Prevents data leakage, reducing the risk and cost of breaches.
- **Strategic Advantage** – Positions organizations ahead in an emerging, high-impact field.

2

A Sustainable and Scalable Financial Model:

Our strong financial strategy is anchored by:

- **Clear Revenue Model** – Establishes a solid foundation for financial sustainability.
- **Detailed Funding Roadmap** – Provides a structured path for growth and scalability.
- **Market-Responsive Growth** – Enables expansion as the market evolves.
- **Long-Term Success** – Positions us to build a sustainable and lasting enterprise.

Expected Impact and Benefits

1

Ethical and Inclusive Data Protection

Our system safeguards the right to privacy, a cornerstone of **ethical technology**. By future-proofing against quantum threats, we protect sensitive data for everyone, including vulnerable groups, ensuring **equitable access to secure healthcare**. The clear detection of attacks fosters trust and accountability, essential for building **secure, transparent infrastructure**.

2

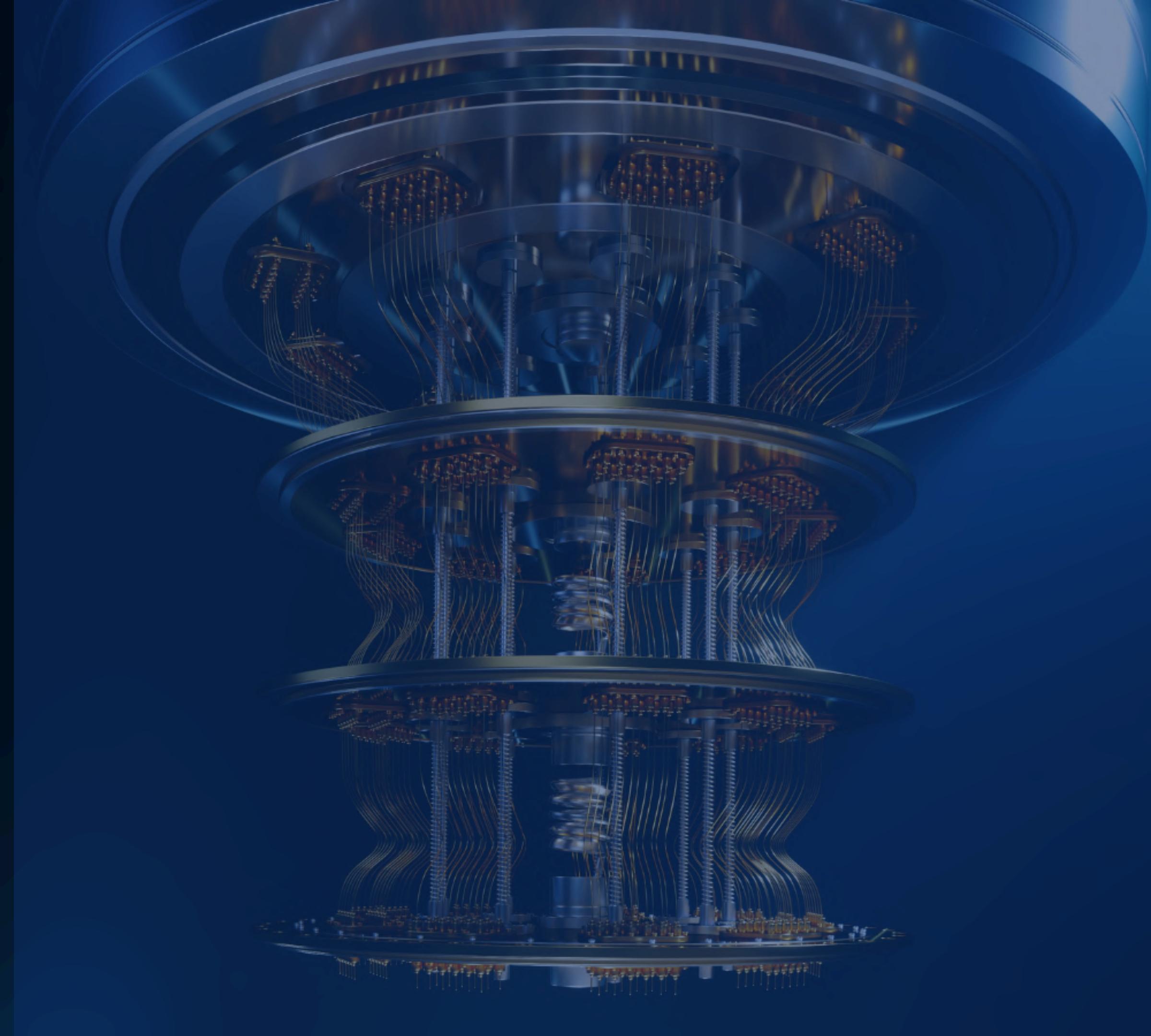
Risk Reduction and Compliance

We **significantly reduce** the **risk** of data breaches, operational downtime, and financial losses, as demonstrated by the disruptions faced by other healthcare providers. Our solution ensures **robust compliance** with major data protection regulations like PDPA (Malaysia), HIPAA, and GDPR.

3

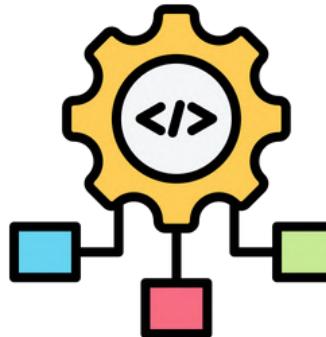
Unrivaled Security and Future Readiness

Our system provides "**Zero Leakage Assurance**" by making intercepted data useless without the correct quantum key. Security is guaranteed by the principles of quantum physics, not computational assumptions, providing a truly **future-proof defense against quantum-era threats**. This positions the hospital as a leader in secure digital healthcare and demonstrates a commitment to long-term data protection.



Resource Requirements

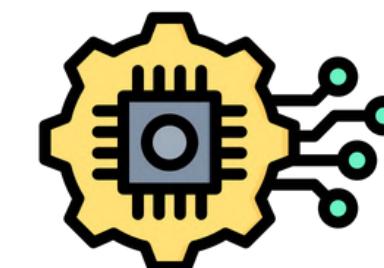
Resource Requirements



Technology Stack

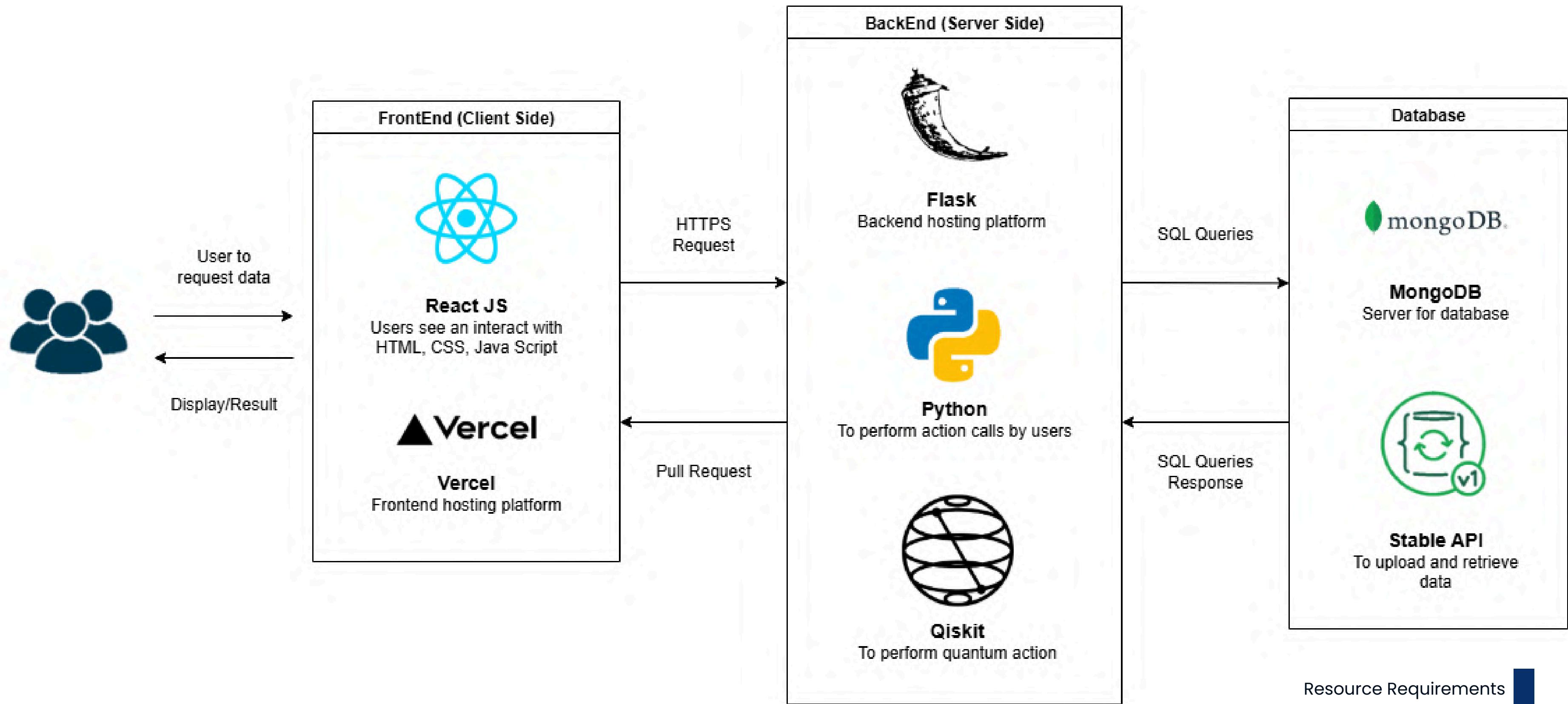


Architecture Diagram

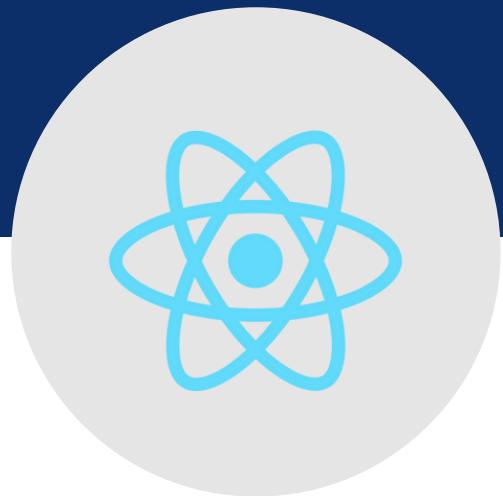


Product Dataflow Diagram

Architecture Diagram



Technology Stack: FrontEnd



React JS

Chosen due to its component-based architecture, which allows for building reusable UI elements.



Vercel

It offers a seamless and high-performance deployment platform optimized for React applications with a global CDN and automatic scaling.

Technology Stack: BackEnd



Flask

A lightweight and flexible web framework for creating the crucial API layer.



Python

General purpose programming language that serve as the core of our application's backend logic.



Qiskit

A crucial component for our quantum functionality.

Technology Stack: Database



MongoDB

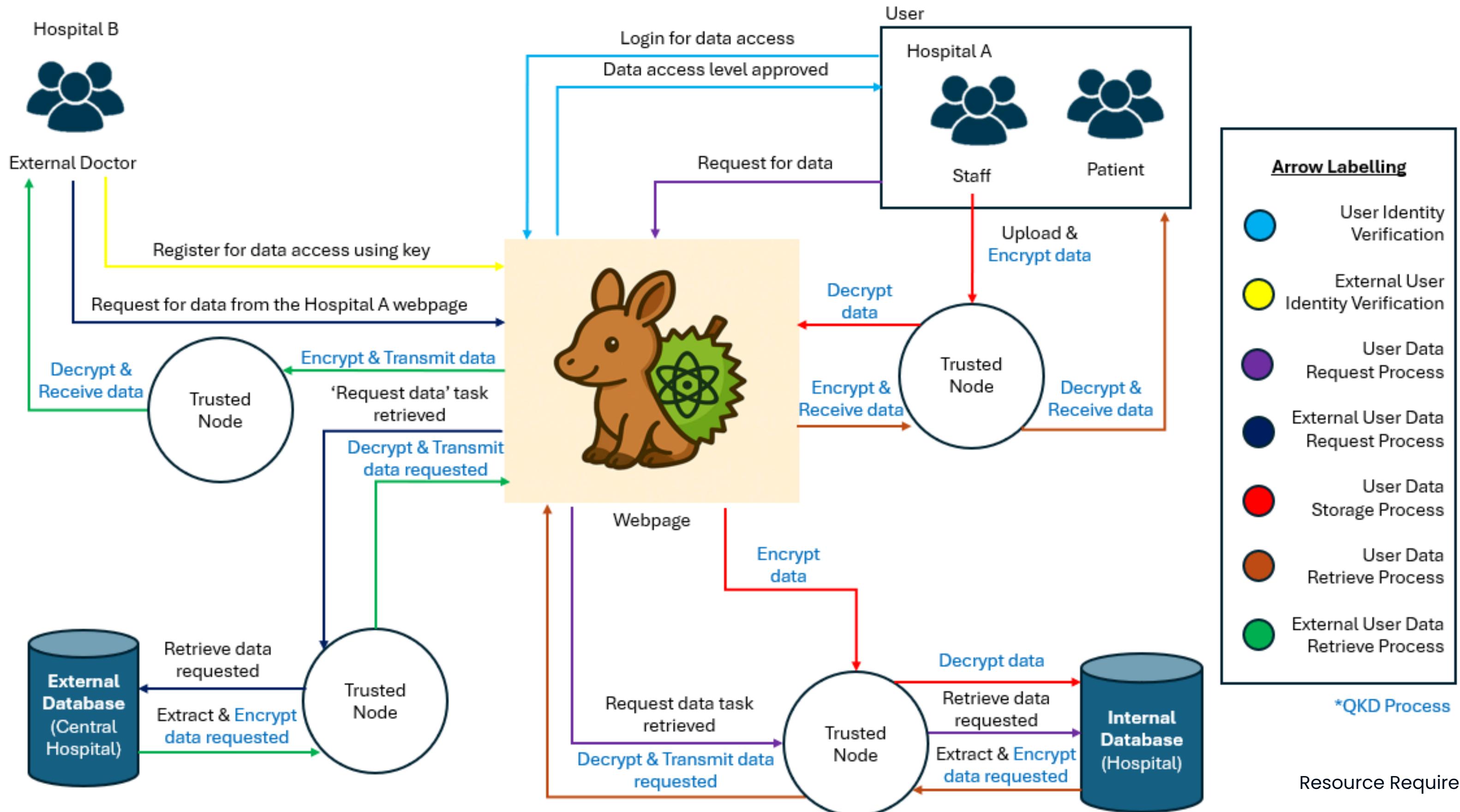
NoSQL document database, as it's the ideal choice for storing and managing the JSON-like data that our system will handle.



StableAPI

A set of protocols that provides a long-term guarantee of backward compatibility, as it's the optimal choice for ensuring seamless, uninterrupted communication between the application and backend.

Product Dataflow Diagram

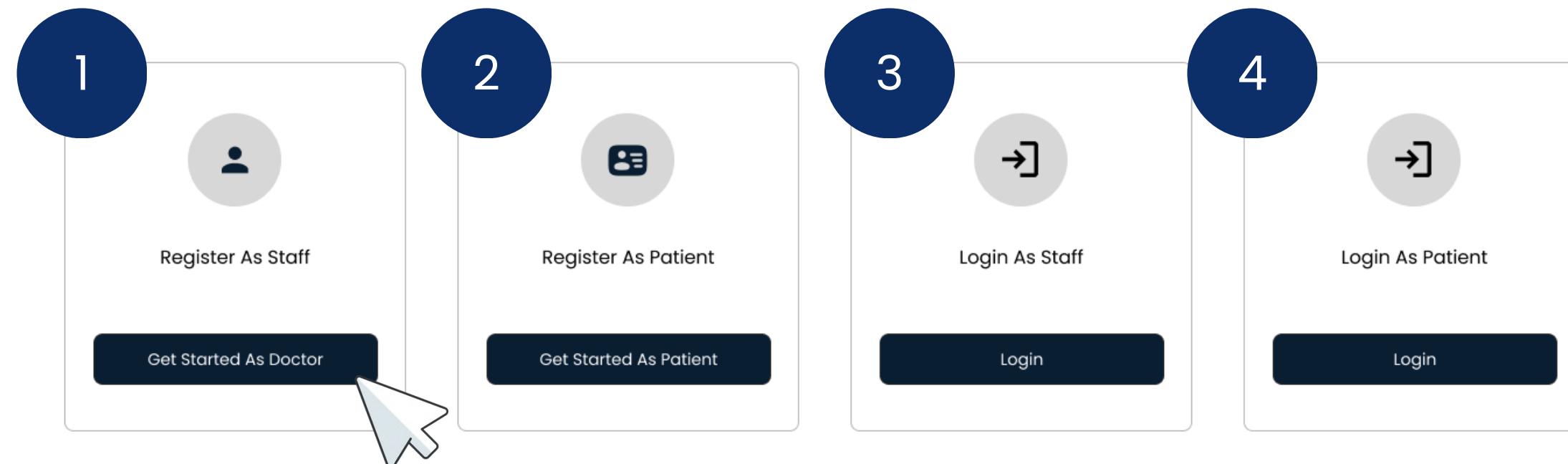
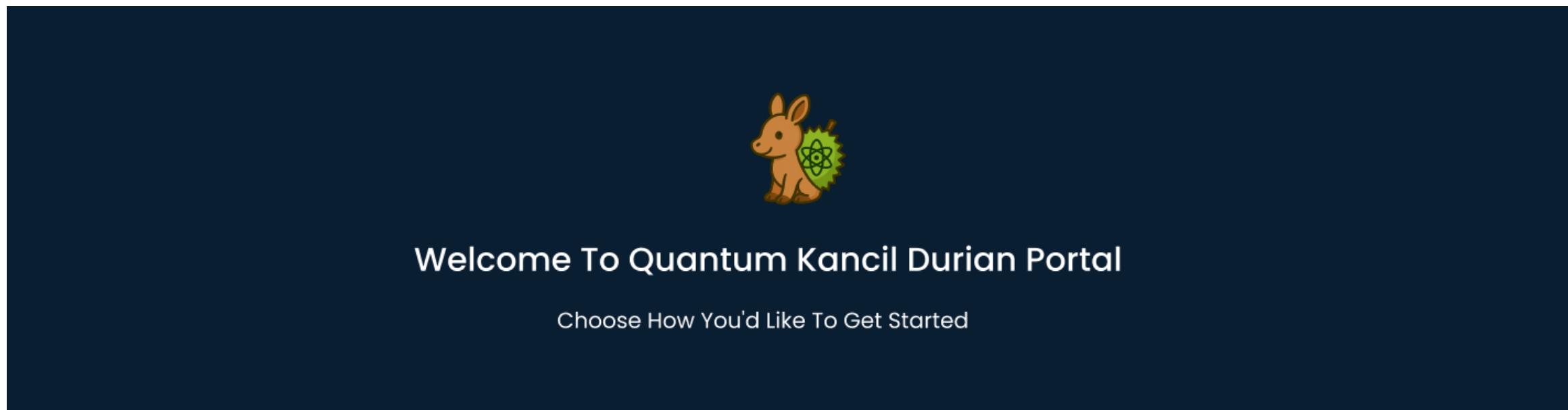




Prototype

Prototype: Home Page

To get started, users can either register for a new account (if they don't have one) or log in with their existing credentials.

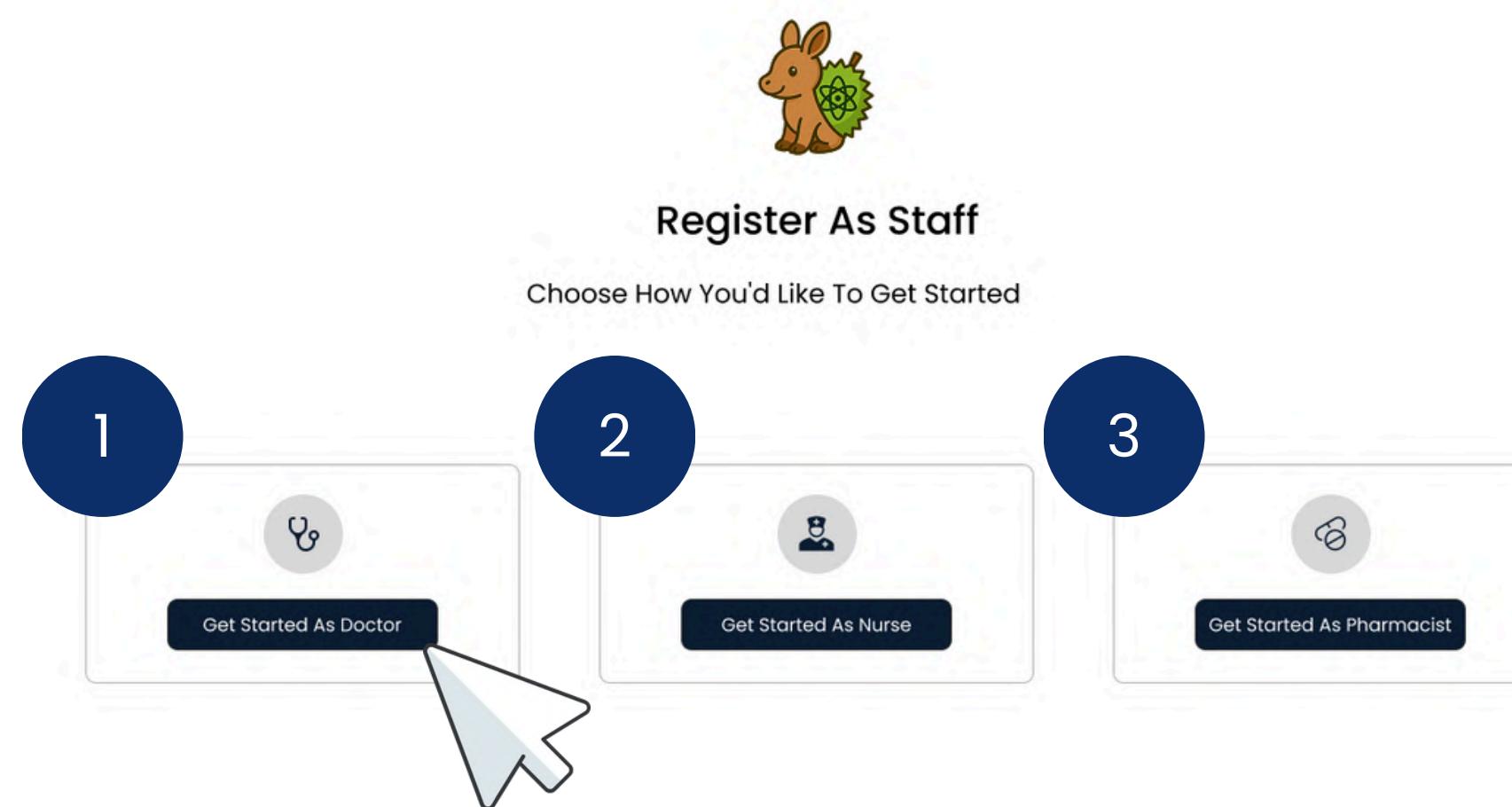


Login/Register

- 1 Register As Staff
- 2 Register As Patient
- 3 Login As Staff
- 4 Login As Patient

Prototype: 'Register As Staff' Path

The system supports different staff user types – Doctors, Nurses, and Pharmacists – each with access to features tailored to their professional role.



Register As Staff

1 Get Started As Doctor

2 Get Started As Nurse

3 Get Started As Pharmacist

Prototype: 'Register As Staff' Path

Register As Staff > Get Started As Doctor
> **Malaysian**



Register As Staff > Get Started As Doctor
> **Non-Malaysian**



Complete Account Setup As Doctor

Malaysian Non-Malaysian

First Name: Adam
Last Name: Smith
Gender: Male Female
NRIC: 900810-09-7878
Citizenship: Malaysia
Staff ID: HOSP12345
Medical Council Registration Number (MMC): MMC123456
Specialization: Cardiology
Current Hospital Name: Thompson Hospital Kota Damansara
Residential Address: 15 Apartment 9A Jalan Van Praagh Taman Continental 11600 Jelutong MYS

Copy of NRIC
Upload your file (PDF only)

Medical Degree Certificate (e.g. MBBS/MD)
Upload your file (PDF only)

Malaysian Medical Council (MMC) Annual Practicing Certificate (APC)
Upload your file (PDF only)

Medical License
Upload your file (PDF only)

Recent Passport-Sized Photo
Upload jpg/png only

Password
Placeholder

Confirm Your Password
Placeholder

Password must be at least 8 Characters and must contain at least a Capital Letter, a Number and a Special Character.

I hereby accept the [T&C](#).

Submit

Complete Account Setup As Doctor

Malaysian Non-Malaysian

First Name: Adam
Last Name: Smith
Gender: Male Female
Passport Number: A12345678
Visa Type: Employment Pass Category II
Citizenship: Malaysia
Staff ID: HOSP12345
Medical Council Registration Number (MMC): MMC123456
Specialization: Cardiology
Current Hospital Name: Thompson Hospital Kota Damansara
Residential Address (Malaysia): 15 Apartment 9A Jalan Van Praagh Taman Continental 11600 Jelutong MYS

Copy of Passport
Upload your file (PDF only)

Visa Document
Upload your file (PDF only)

Medical Degree Certificate (e.g. MBBS/MD)
Upload your file (PDF only)

Malaysian Medical Council (MMC) Annual Practicing Certificate (APC)
Upload your file (PDF only)

Medical License
Upload your file (PDF only)

Recent Passport-Sized Photo
Upload jpg/png only

Password
Placeholder

Confirm Your Password
Placeholder

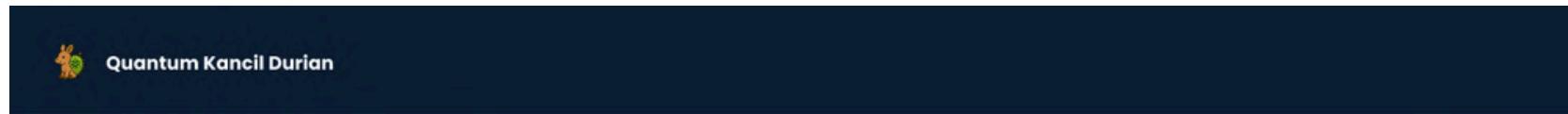
Password must be at least 8 Characters and must contain at least a Capital Letter, a Number and a Special Character.

I hereby accept the [T&C](#).

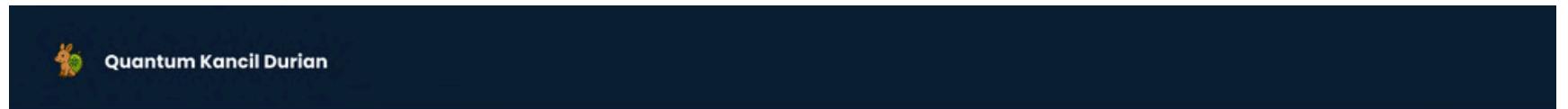
Submit

Prototype: 'Register As Staff' Path

Register As Staff > Get Started As Nurse
> **Malaysian**



Register As Staff > Get Started As Nurse
> **Non-Malaysian**



Prototype: 'Register As Staff' Path

Register As Staff > Get Started As Pharmacist
> **Malaysian**



Register As Staff > Get Started As Pharmacist
> **Non-Malaysian**



Prototype: 'Register As Staff' Path

Register As Staff > Get Started As Doctor/Nurse/Pharmacist > Malaysian/Non-Malaysian
> **Complete Account Login**

The image displays two side-by-side screenshots of a mobile application's 'Complete Account Login' screen. Both screenshots show a header bar with a logo and the text 'Quantum Kancil Durian'. Below the header is a circular profile picture placeholder.

Left Screenshot (Step 1 of 2):

- Header:** Complete Account Login, Step 1 of 2.
- Information Bar:** A grey bar with a lock icon and the text: "We take privacy issues seriously. You can be sure that your personal data is securely protected." with a close button (X).
- Email Address Input:** An input field containing "adam@hoskd.com".
- Password Input:** An input field labeled "Placeholder".
- Forgot Password Link:** "Forgot your Password?"
- Login Button:** A dark blue button labeled "Login".

Right Screenshot (Step 1 of 2):

- Header:** Complete Account Login.
- Information Bar:** A grey bar with a lock icon and the text: "We take privacy issues seriously. You can be sure that your personal data is securely protected." with a close button (X).
- Text:** "Enter 6-Digit Code Sent To +6011-XXX-XXXX."
- Code Input:** Six empty input fields for entering the code.
- Text:** "Code Expires In 30s." and a "Send again." button.
- Verify & Continue Button:** A dark blue button labeled "Verify & Continue".

Prototype: 'Register As Patient' Path

Patients are registered separately, using the same portal but with a dedicated interface.

Register As Patient > **Malaysian**



Register As Patient > **Non-Malaysian**



Prototype: 'Register As Patient' Path

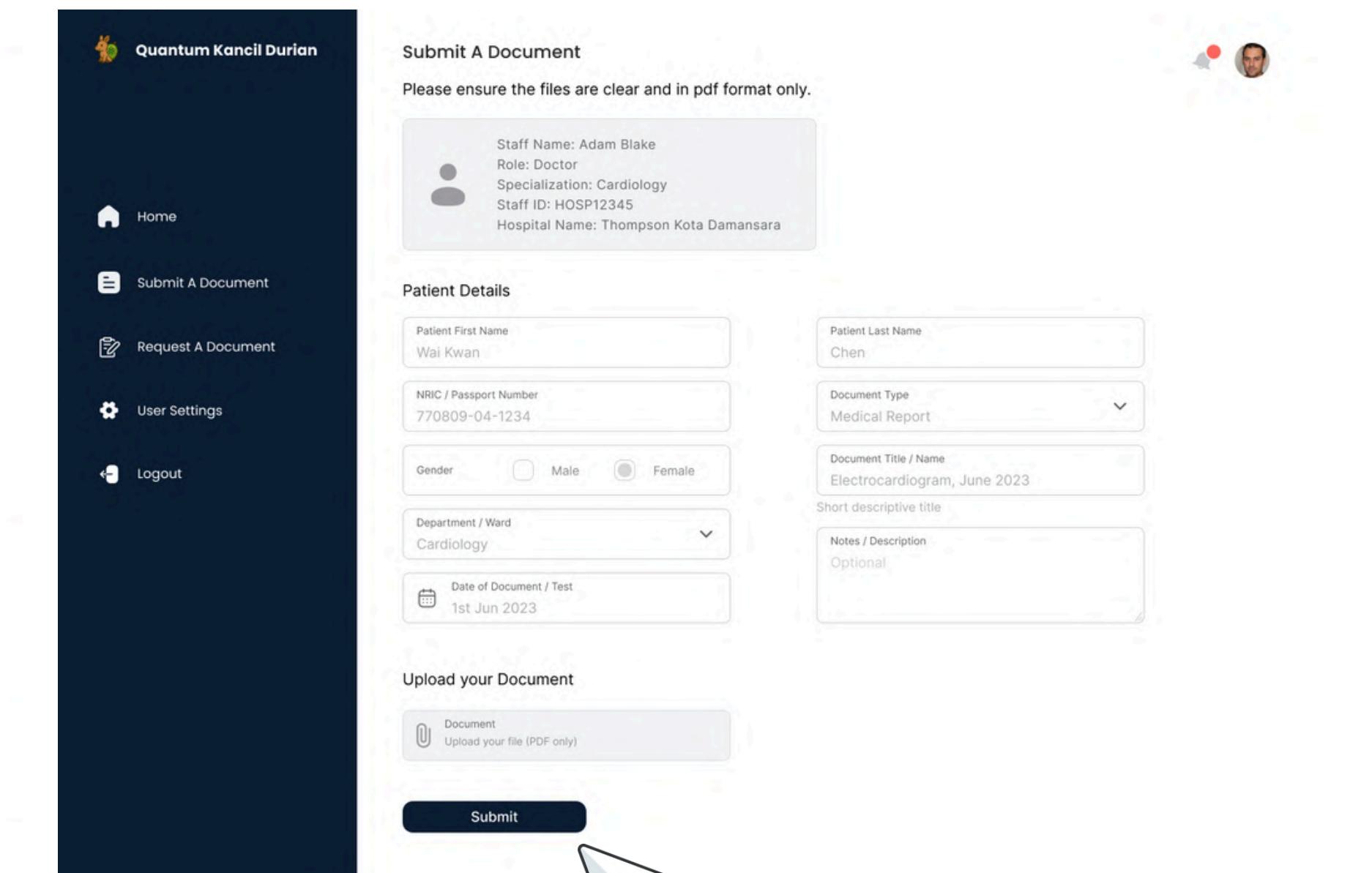
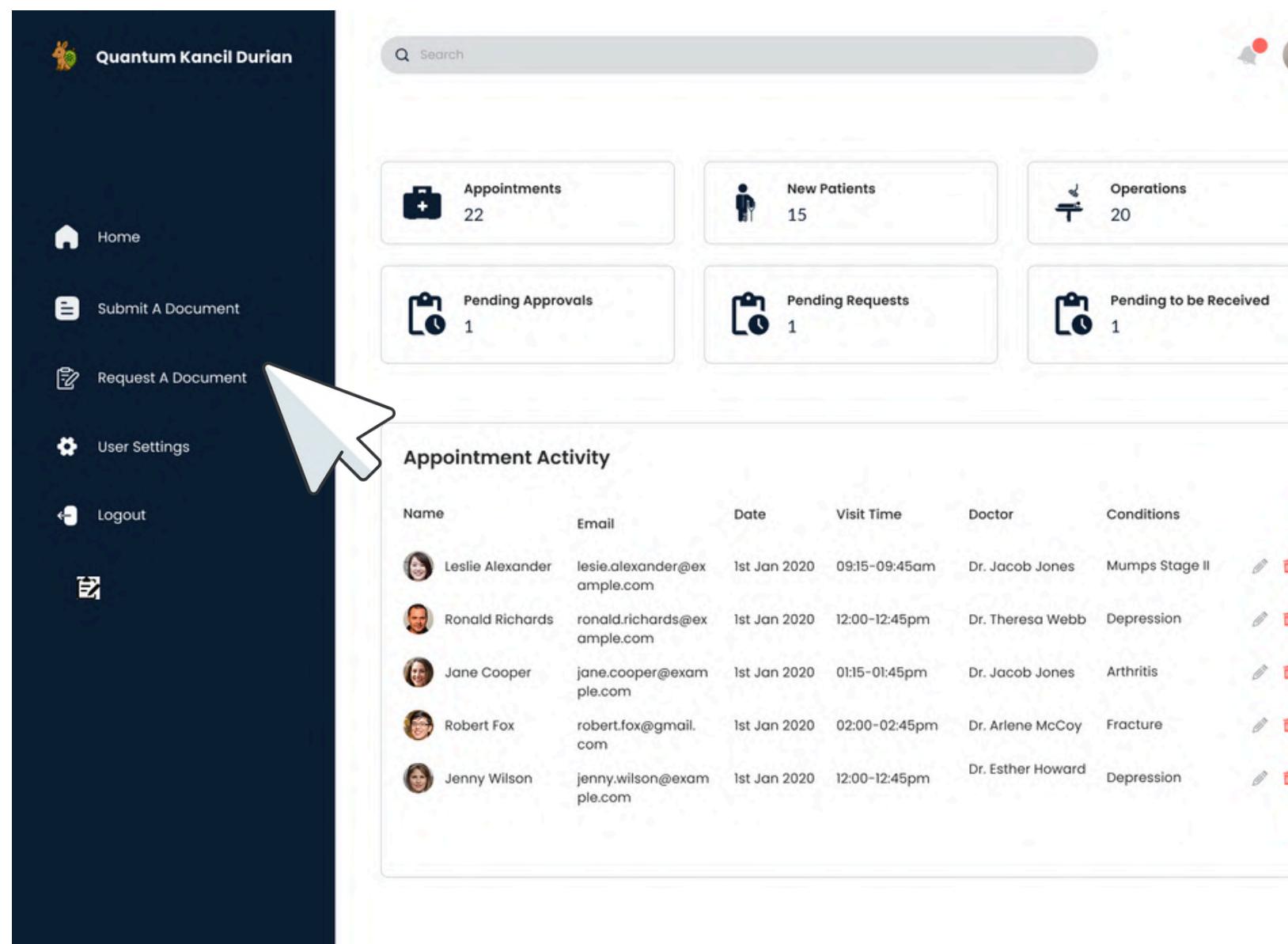
Register As Patient > Malaysian/Non-Malaysian > **Complete Account Login**

A diagram showing the transition from the first step to the second step. A curved arrow points from the "Login" button on the left screenshot to the "Verify & Continue" button on the right screenshot. A large blue cursor arrow points from the "Login" button towards the "Verify & Continue" button.

Prototype: Functions

Staff members who need to upload documents such as lab reports or test results can do so through the "Submit a Document" section in the menu.

Login As Staff > **Staff Home Page** > **Submit A Document**



Quantum Kancil Durian

Search

Appointments 22

New Patients 15

Operations 20

Pending Approvals 1

Pending Requests 1

Pending to be Received 1

Home

Submit A Document

Request A Document

User Settings

Logout

Appointment Activity

| Name | Email | Date | Visit Time | Doctor | Conditions | Action | |
|------------------|------------------------------|--------------|---------------|-------------------|----------------|--------|--|
| Leslie Alexander | leslie.alexander@example.com | 1st Jan 2020 | 09:15-09:45am | Dr. Jacob Jones | Mumps Stage II | | |
| Ronald Richards | ronald.richards@example.com | 1st Jan 2020 | 12:00-12:45pm | Dr. Theresa Webb | Depression | | |
| Jane Cooper | jane.cooper@example.com | 1st Jan 2020 | 01:15-01:45pm | Dr. Jacob Jones | Arthritis | | |
| Robert Fox | robert.fox@gmail.com | 1st Jan 2020 | 02:00-02:45pm | Dr. Arlene McCoy | Fracture | | |
| Jenny Wilson | jenny.wilson@example.com | 1st Jan 2020 | 12:00-12:45pm | Dr. Esther Howard | Depression | | |

Quantum Kancil Durian

Submit A Document

Please ensure the files are clear and in pdf format only.

Staff Name: Adam Blake
Role: Doctor
Specialization: Cardiology
Staff ID: HOSP12345
Hospital Name: Thompson Kota Damansara

Patient Details

Patient First Name: Wai Kwan
Patient Last Name: Chen
NRIC / Passport Number: 770809-04-1234
Gender: Male Female
Document Type: Medical Report
Document Title / Name: Electrocardiogram, June 2023
Short descriptive title:
Notes / Description: Optional
Date of Document / Test: 1st Jun 2023

Upload your Document

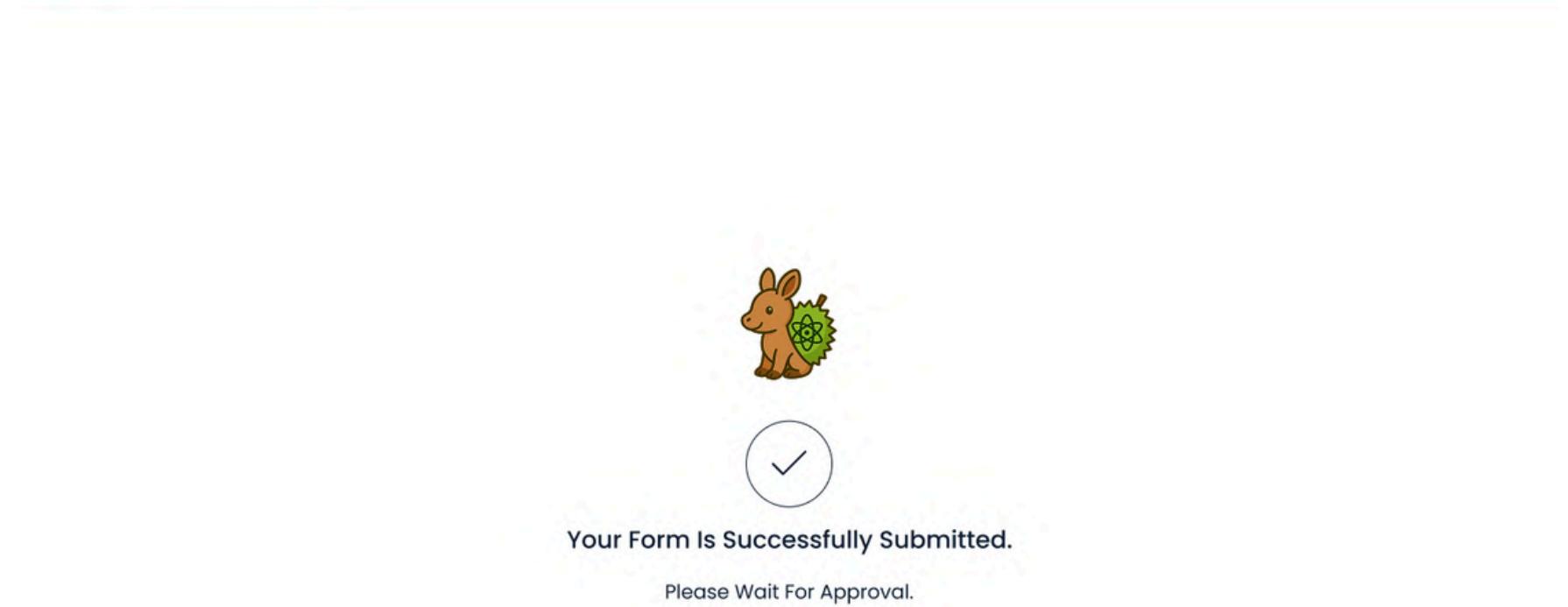
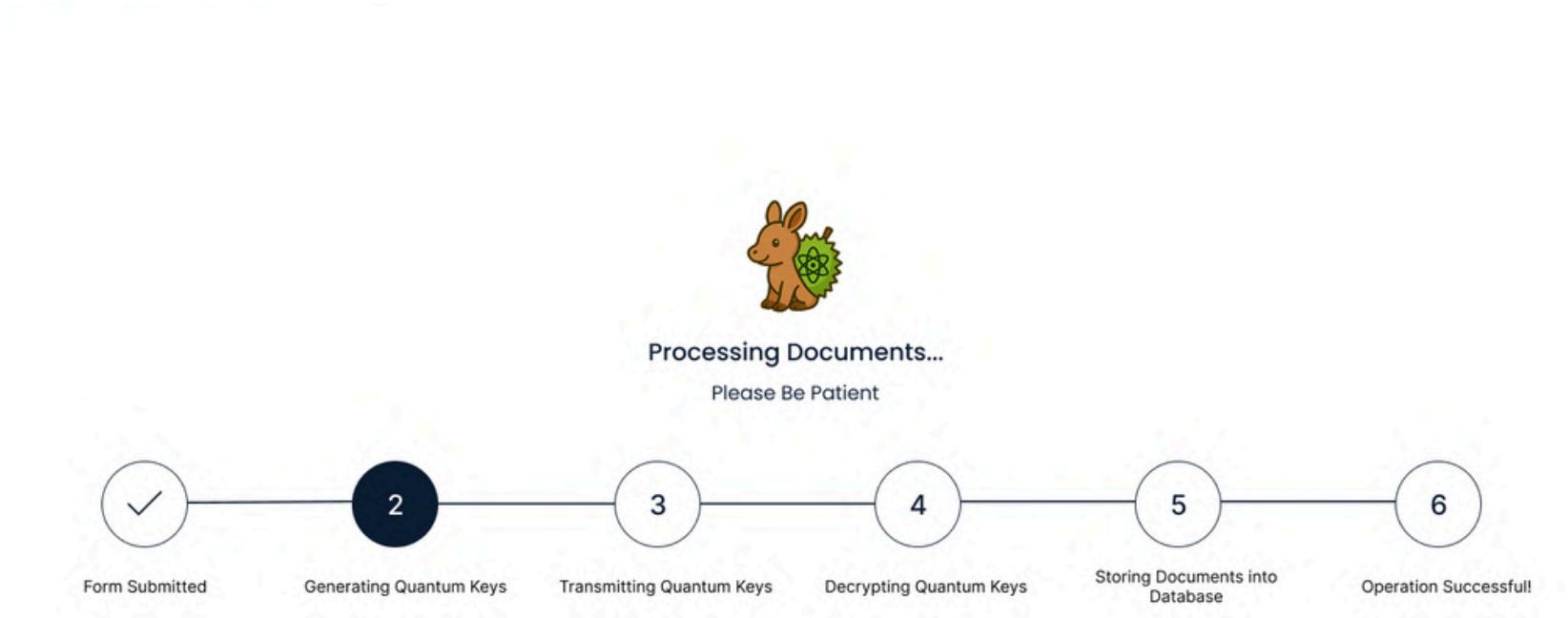
Document: Upload your file (PDF only)

Submit

Prototype

Prototype: Functions

Login As Staff > Staff Home Page > Submit A Document > **Processing Documents** > **Submitted Successfully**



Prototype: Functions

Doctors and nurses can also request patient documents, such as lab reports from other departments, through the “Request a Document” section.

Login As Staff > Staff Home Page > **Request A Document** > **Submitted Successfully**

Quantum Kancil Durian

Request A Document

Staff Name: Adam Blake
Role: Doctor
Specialization: Cardiology
Staff ID: HOSP12345
Hospital Name: Thompson Kota Damansara

Requesting Patient Details

Patient First Name: Hui Ling
Patient Last Name: Tan
NRIC / Passport Number: 990703-08-2342
Gender: Male Female

Requesting Information

Department: Neurology
Staff Name: Adam Smith
Staff ID: HOSP12333
Document Type: Medical Report
Document Title / Name: MRI Brain Scan, June 2023
Reason for Request: Continuity of Care

Submit

Your Form Is Successfully Submitted.
Please Wait For Approval.

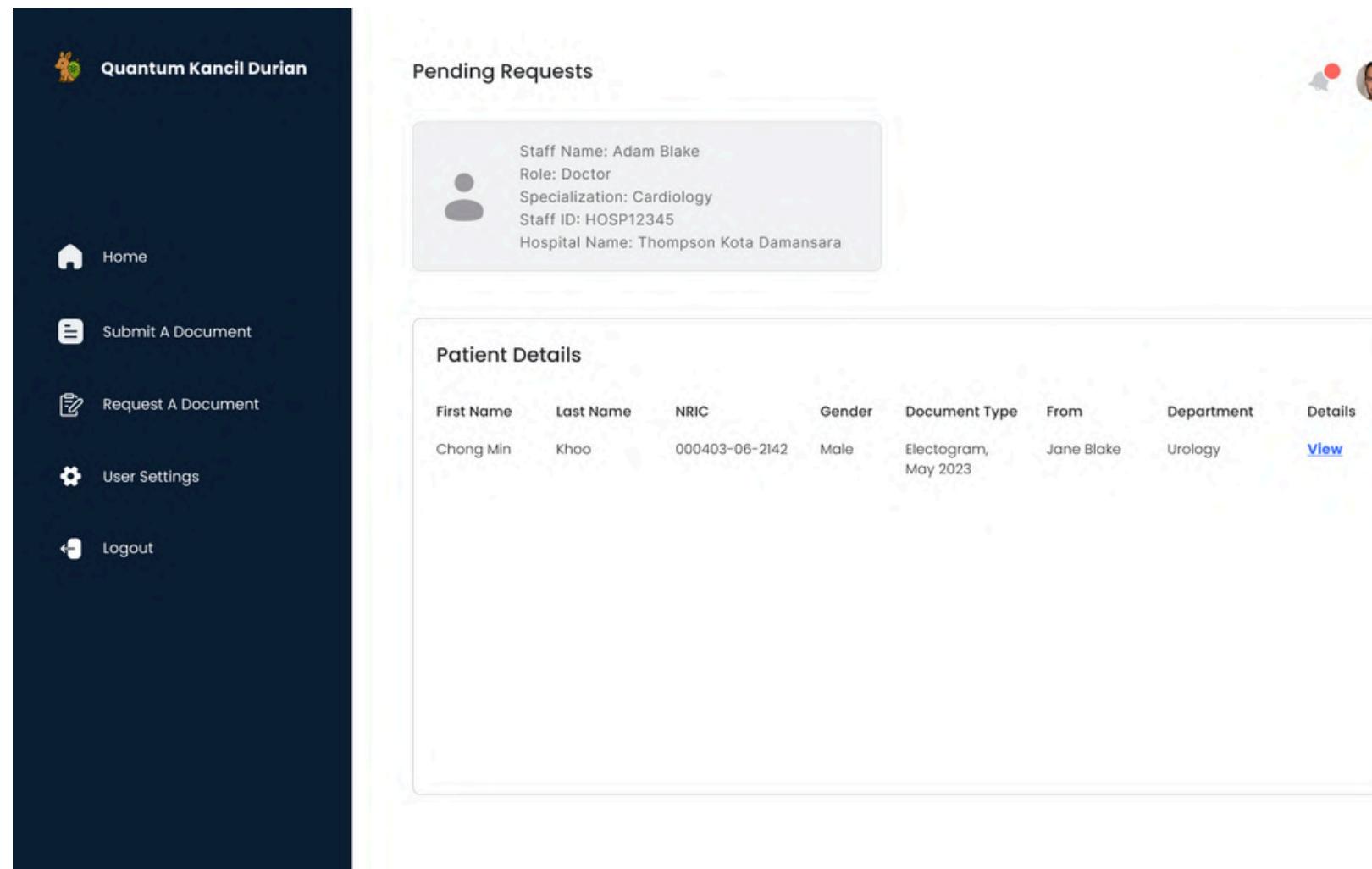
Quantum Kancil Durian

A cartoon deer holding a green checkmark.

Prototype: Functions

The “Pending Requests” section displays document requests received from other departments, while the “Pending Approvals” section lets staff monitor the progress of documents they have requested from other departments. Both options can be accessed directly from the home page for quick navigation.

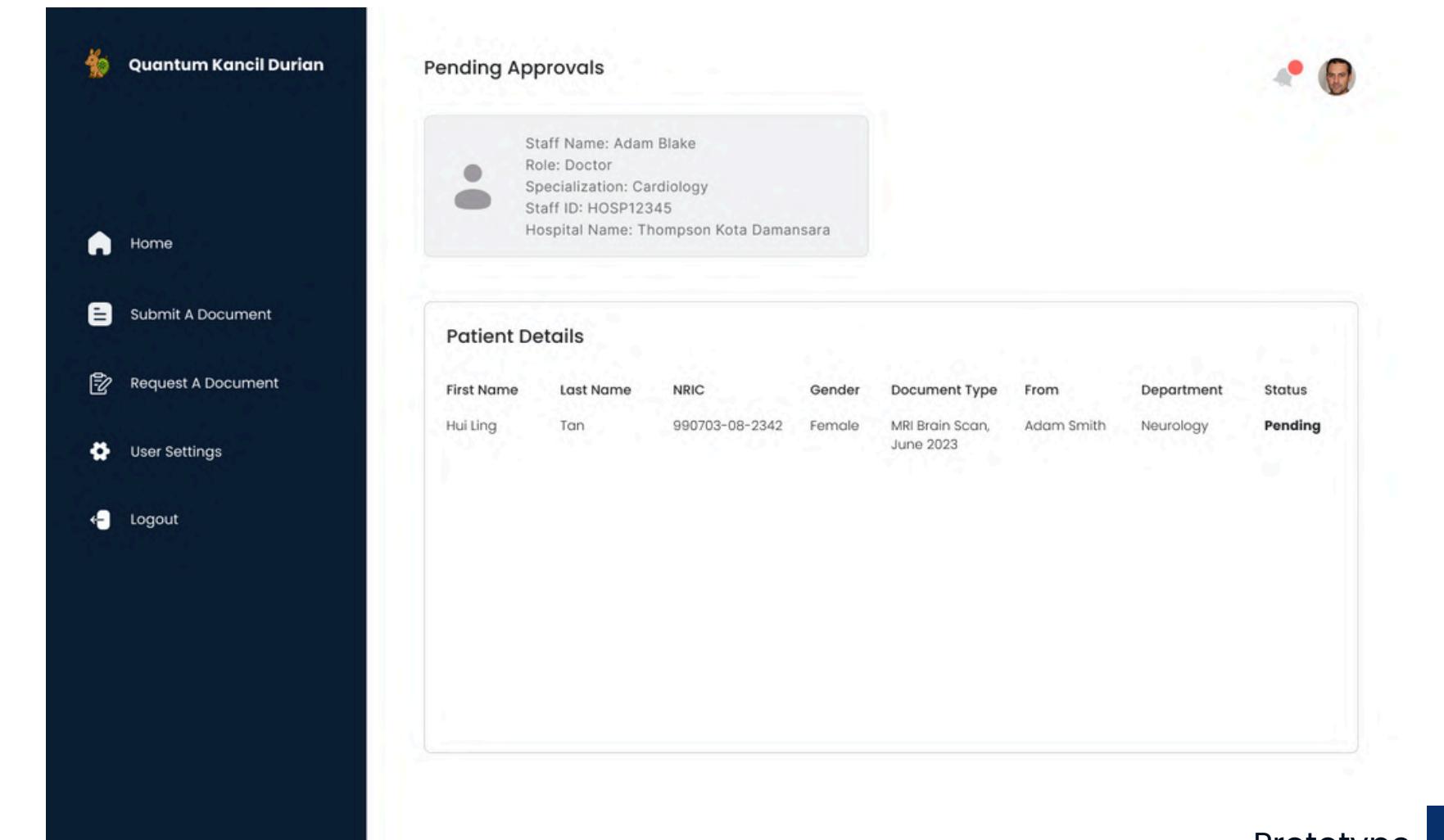
Login As Staff > Staff Home Page
> **Pending Requests**



This screenshot shows the 'Pending Requests' section of the staff home page. At the top, there's a summary box for a request from Adam Blake. Below it, a table displays patient details for Chong Min Khoo, including first name, last name, NRIC, gender, document type, source, department, and a 'View' link.

| First Name | Last Name | NRIC | Gender | Document Type | From | Department | Details |
|------------|-----------|----------------|--------|----------------------|------------|------------|----------------------|
| Chong Min | Khoo | 000403-06-2142 | Male | Electogram, May 2023 | Jane Blake | Urology | View |

Login As Staff > Staff Home Page
> **Pending Approvals**



This screenshot shows the 'Pending Approvals' section of the staff home page. At the top, there's a summary box for a request from Adam Blake. Below it, a table displays patient details for Hui Ling Tan, including first name, last name, NRIC, gender, document type, source, department, and status.

| First Name | Last Name | NRIC | Gender | Document Type | From | Department | Status |
|------------|-----------|----------------|--------|---------------------------|------------|------------|----------------|
| Hui Ling | Tan | 990703-08-2342 | Female | MRI Brain Scan, June 2023 | Adam Smith | Neurology | Pending |

Prototype: Functions

The “Pending to be Received” section displays all approved requests and allows staff to view documents shared by other departments. This option is also accessible directly from the home page.

Login As Staff > Staff Home Page > Request a Document > Pending Requests > **Pending to be Received** > **Retrieving Documents**

The screenshot displays two main sections of the Quantum Kancil Durian staff interface:

- Left Panel (Staff Home Page):** A sidebar with a dark blue background and white icons. It includes links for Home, Submit A Document, Request A Document, User Settings, and Logout. The title "Quantum Kancil Durian" is at the top.
- Middle Panel (Pending to be Received):** A card titled "Pending to be Received" showing details for a staff member: Adam Blake (Role: Doctor, Specialization: Cardiology, Staff ID: HOSP12345, Hospital Name: Thompson Kota Damansara). Below this is a "Patient Details" table:

| First Name | Last Name | NRIC | Gender | Document Type | From | Department | Details |
|------------|-----------|----------------|--------|--------------------------|------------|------------|----------------------|
| Yashvi | M. Patel | 040910-08-1044 | Female | MRI Brain Scan, Dec 202X | Hiren Shah | Neurology | View |

- Right Panel (Retrieving Documents):** A progress bar titled "Retrieving Documents..." with a sub-instruction "Please Be Patient". The process is divided into six numbered steps: 1 (Request Submitted), 2 (Retrieving Data), 3 (Generating Quantum Keys), 4 (Transmitting Quantum Keys), 5 (Decrypting Quantum Keys), and 6 (Operation Successful!). A "View the Document" button is located at the bottom right of this panel.

Prototype: Functions

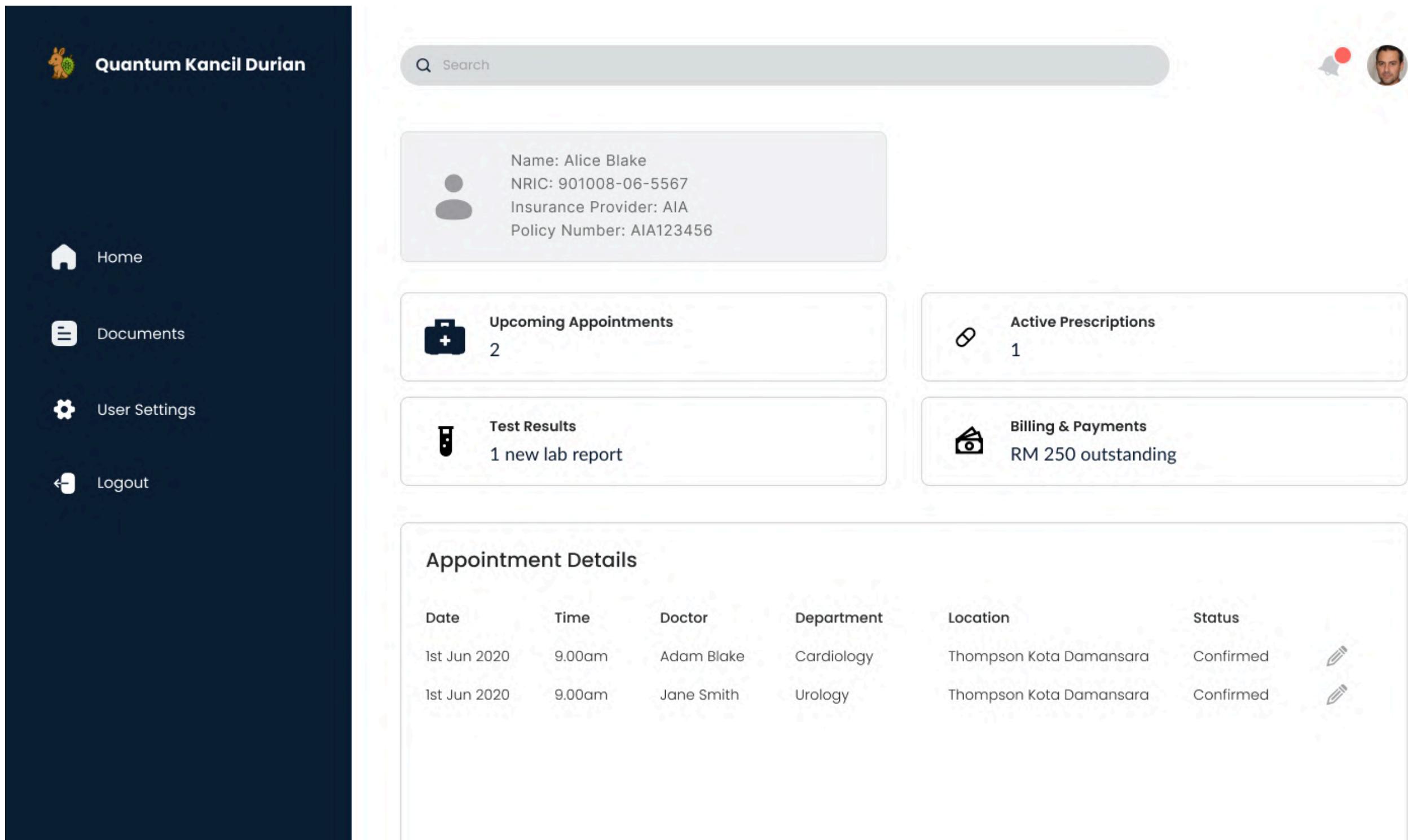
Shared documents can be downloaded as PDF files and are automatically watermarked to ensure transparency and traceability.

Login As Staff > Staff Home Page > Request a Document > Pending Requests > Pending to be Received
> Retrieving Documents > **Download as PDF**

The screenshot shows a web-based medical report viewer. At the top, there's a dark header bar with the logo 'Quantum Kancil Durian' and a 'Download as PDF' button. Below the header, patient information is displayed: Yashvi M. Patel (Age: 21 Years, Sex: Female), PID: 555, Apt ID: 2025252, Ref. By: Dr. Hiren Shah. To the right of this information is a large, semi-transparent watermark of a hand holding a pen, with the text 'Imaging Center' faintly visible behind it. The main content area is titled 'MRI BRAIN'. It contains a detailed description of a brain scan, mentioning an extra axial hematoma and providing diagnostic points. Below the text are two grids of small MRI slices. At the bottom of the page, there are footer links for 'Thanks for Reference', 'End of Report', and signatures for 'Dr. Raval Shah' and 'Dr. Vimal Shah'.

Prototype: Patients Home Page

On the patient home page, users can view their upcoming appointments, newly available lab reports, pending bills, and active prescriptions.



The image shows a prototype of a Patient Home Page. On the left, there is a dark sidebar with a logo of a rabbit and the text "Quantum Kancil Durian". The sidebar contains links for "Home", "Documents", "User Settings", and "Logout". The main content area has a light background. At the top right, there is a search bar, a notification icon with a red dot, and a user profile picture. Below the header, a box displays personal information: Name: Alice Blake, NRIC: 901008-06-5567, Insurance Provider: AIA, Policy Number: AIA123456. The main content is organized into four cards: "Upcoming Appointments" (2), "Active Prescriptions" (1), "Test Results" (1 new lab report), and "Billing & Payments" (RM 250 outstanding). At the bottom, a larger box titled "Appointment Details" lists two appointments:

| Date | Time | Doctor | Department | Location | Status | Action |
|--------------|--------|------------|------------|-------------------------|-----------|--------|
| 1st Jun 2020 | 9.00am | Adam Blake | Cardiology | Thompson Kota Damansara | Confirmed | |
| 1st Jun 2020 | 9.00am | Jane Smith | Urology | Thompson Kota Damansara | Confirmed | |

Prototype: Functions

Patients can access all their medical records, including lab reports and test results, through the "Documents" section in the menu.

Login As Patient > **Patient Home Page > Documents > Retrieving Documents > Download as PDF**

The screenshot shows the Patient Home Page with a dark blue header featuring the logo 'Quantum Kancil Durian'. The main content area has a light gray background. On the left, there is a vertical sidebar with icons for Home, Documents, User Settings, and Logout. The main area is titled 'Documents' and contains two sections: 'New Documents' and 'Past Documents'. Each section has a table with columns: Document Title, Document Type, Doctor, Department, Report Date, Notes, and Details (with a 'View' link). A cursor icon is positioned over the 'View' link in the 'New Documents' section. In the top right corner, there is a user profile icon with a red notification dot and a small circular photo of a man.

New Documents

| Document Title | Document Type | Doctor | Department | Report Date | Notes | Details |
|-----------------------|---------------|------------|------------|--------------|--------------------|----------------------|
| MRI Brain Scan Report | Imaging | Adam Blake | Neurology | 1st Jun 2020 | Follow-up required | View |

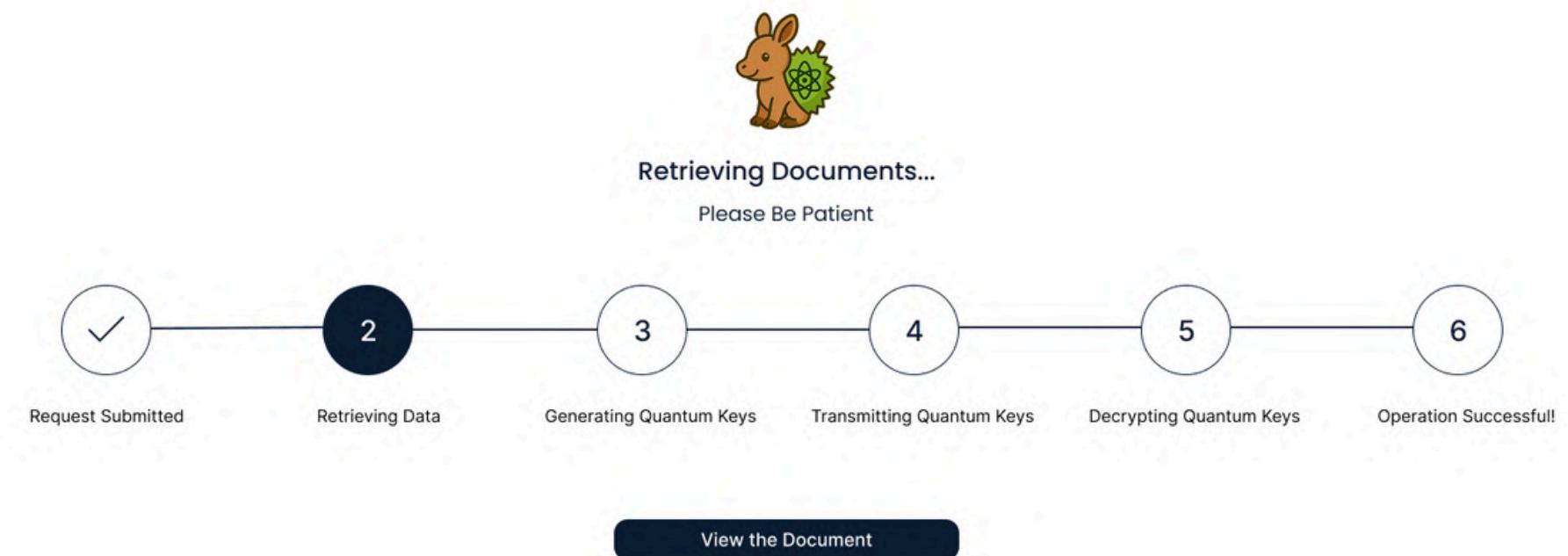
Past Documents

| Document Title | Document Type | Doctor | Department | Report Date | Notes | Details |
|-----------------------|---------------|------------|------------|--------------|-------|----------------------|
| MRI Brain Scan Report | Imaging | Kent Smith | Neurology | 1st Jan 2020 | Fine | View |
| Electrogram | Report | Adam Blake | Cardiology | 1st May 2020 | Fine | View |

Prototype

Prototype: Functions

Login As Patient > **Patient Home Page** > **Documents** > **Retrieving Documents** > **Download as PDF**



Quantum Kancil Durian

Download as PDF

Yashvi M. Patel
Age : 21 Years
Sex : Female

PID : 555
Apt ID : 2025252
Ref. By : Dr. Hiren Shah

Registered on:
02:31 PM 02 Dec, 2X
Reported on:
04:35 PM 02 Dec, 2X

MRI BRAIN

A well defined extra axial (elliptical or crescentic shaped) hematoma is seen in the (Mention the site of the lesion). It showed Mention the signal changes in T1 and T2WIs as described with the intra cerebral hematoma however,

- The subdural hematoma may show sedimentation level, then you mention the signal changes of its upper and lower components.
- No edema is present in cases of epidural or subdural hematoma.
- No hemosiderin seen in these cases [usually].

Sub arachnoid hemorrhage is not assessed by MRI, if so, you can follow the same items used for CT and remember to change the densities to signal intensities.

- Fresh blood signal is seen smearing the cortical sulci and extra axial CSF spaces
- Extension into the ventricular system showing dark signal in T2 WIs
- Also mention that the ventricular system is dilated denoting the presence of communicating hydrocephalus which is usually seen in cases of subarachnoid hemorrhage.
- Normal posterior fossa (if the lesion is not in the posterior fossa).
- Scanned paranasal sinuses are clear.

Imaging Center

Thanks for Reference

******End of Report******

Dr. Payal Shah
(MSC, PGDM)

Dr. Vimal Shah
(MD, Radiologist)

A detailed 3D rendering of a quantum computing system. It features several concentric rings of blue and gold-colored components, likely superconducting qubits or readout electronics. Numerous thin, glowing yellow lines represent the qubit wires connecting different parts of the machine. The overall design is intricate and futuristic, set against a dark blue background.

Future Work

Future Works: Security Issues

Since the security is not 100% guaranteed in the protocol, we propose:



Information Reconciliation

Act as an error correction process in the post QKD. It detects and corrects the inconsistencies between two generated keys by distilling a secure key from noisy material or a channel.



Privacy Amplification

Act as an eavesdropper information remover in the post QKD process. It distills the raw keys that are correlated with the eavesdropper into a highly secure key.



References

References

- Experian. Protect patient identities. Available at: <https://www.experian.com/healthcare/products/protect-patient-identities> (Accessed: 8 September 2025).
- CodeBlue. Malaysia Patient Data Leak Came From Private Entity. Available at: <https://codeblue.galencentre.org/2019/10/malaysia-patient-data-leak-came-from-private-entity-moh-says/#:~:text=In%20September%2C%20Greenbone%20revealed%20that,Imaging%20and%20Communications%20in%20Medicine> (Accessed: 8 September 2025).
- Bank Info Security. Hackers Steal 17M Patient Records in Attack on 3 Hospitals. Available at: <https://www.bankinfosecurity.com/hackers-steal-17m-patient-records-in-attack-on-3-hospitals-a-27059> (Accessed: 8 September 2025).
- GHP News. The Average Cost of a Data Breach in the Healthcare Sector. Available at: <https://ghpnews.digital/the-average-cost-of-a-data-breach-in-the-healthcare-sector-is-9-77-million-a-staggering-67-percent-higher-than-the-global-average-of-4-88-million/> (Accessed: 8 September 2025).
- CHUBB. Cyber insurance for the healthcare industry. Available at: <https://www.chubb.com/my-en/articles/business/cyber-insurance-for-the-healthcare-industry.html> (Accessed: 8 September 2025).
- Fortune Business Insights. Healthcare Cybersecurity Market. Available at: <https://www.fortunebusinessinsights.com/healthcare-cybersecurity-market-110389> (Accessed: 8 September 2025).
- Precedence Research. Healthcare Cybersecurity Market Size, Share, and Trends. Available at: <https://www.precedenceresearch.com/healthcare-cybersecurity-market> (Accessed: 8 September 2025).
- ID Quantique (2020, December 10). FragmentiX quantum-safe storage solution [Press release]. Available at: https://marketing.idquantique.com/acton/attachment/11868/f-2b39fb7a-37d5-436a-9b20-49f95100585a/1/-/-/-/IDQ-fragmentiX_pressrelease_OpenQKD_2020-12-10_EN.pdf (Accessed: 8 September 2025).

References

- University of Science and Technology of China. Beijing-Shanghai Quantum Communication Network Put into Use (2017, September 1). Available at: <https://en.ustc.edu.cn/info/1110/3630.htm> (Accessed: 8 September 2025).
- University of Science and Technology of China. USTC Develops Quantum Microsatellite and Achieves Real-Time Quantum Key Distribution Between Microsatellite and Mobile Ground Stations (2025, March 20). Available at: <https://en.ustc.edu.cn/info/1007/5032.htm> (Accessed: 8 September 2025).
- Quantum Computing Inc. Secures Purchase Order from Top 5 U.S. Bank to Advance Quantum Cybersecurity Testbed. Available at: <https://quantumcomputinginc.com/news/press-releases/quantum-computing-inc.-secures-purchase-order-from-top-5-u.s.-bank-to-advance-quantum-cybersecurity-testbed> (Accessed: 8 September 2025).
- Toshiba. BT and Toshiba to build world's first quantum-secured commercial metro network across London. Available at: <https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/bt-and-toshiba-to-build-worlds-first-quantum-secured-commercial-metro-network-across-london> (Accessed: 8 September 2025).
- EY. BT and Toshiba launch first commercial trial of quantum secured communication services – EY becomes first commercial customer. Available at: https://www.ey.com/en_uk/newsroom/2022/04/bt-and-toshiba-launch-first-commercial-trial-of-quantum-secured-communication-services (Accessed: 8 September 2025).
- UK Government. National Quantum Strategy Missions (2023). Available at: <https://www.gov.uk/government/publications/national-quantum-strategy/national-quantum-strategy-missions> (Accessed: 8 September 2025).
- Celerity. Quantum Computing and Healthcare Cybersecurity. Available at: <https://celerity-uk.com/resources/quantum-computing-and-healthcare-cybersecurity-why-nhs-leaders-must-act-now> (Accessed: 8 September 2025).
- Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560, 7-11.

References

- Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical review letters*, 67(6), 661.
- Garapo, K., Mafu, M., & Petruccione, F. (2016). Intercept-resend attack on six-state quantum key distribution over collective-rotation noise channels. *Chinese Physics B*, 25(7), 070303.
- HHQ. New Data Breach Notification Requirements under the Personal Data Protection (Amendment) Act 2024. Available at: <https://hhq.com.my/posts/new-data-breach-notification-requirements-under-the-personal-data-protection-amendment-act-2024-5-key-takeaways-for-compliance/#:~:text=The%20consequences%20of%20non%2Dcompliance%20under%20the%20Personal,to%20two%20years%2C%20or%20both%2C%20upon%20conviction>. (Accessed 8 Sep 2025)
- Palo Alto Networks. What Is the California Consumer Privacy Act (CCPA). Available at: <https://www.paloaltonetworks.com/cyberpedia/ccpa> (Accessed 8 Sep 2025)
- Roedl. Updates on Personal Data Protection. Available at: <https://www.roedl.com/insights/newsflash-asean/2022-03/singapore-updates-personal-data-protection#:~:text=Page%20Content,in%20compliance%20with%20the%20PDPA>. (Accessed 8 Sep 2025)