

A Collaborative Approach to Enhance Digital Immunity & Cybersecurity Resilience in eHealth

以協作為核心：強化醫健通數位免疫力與網絡安全韌性

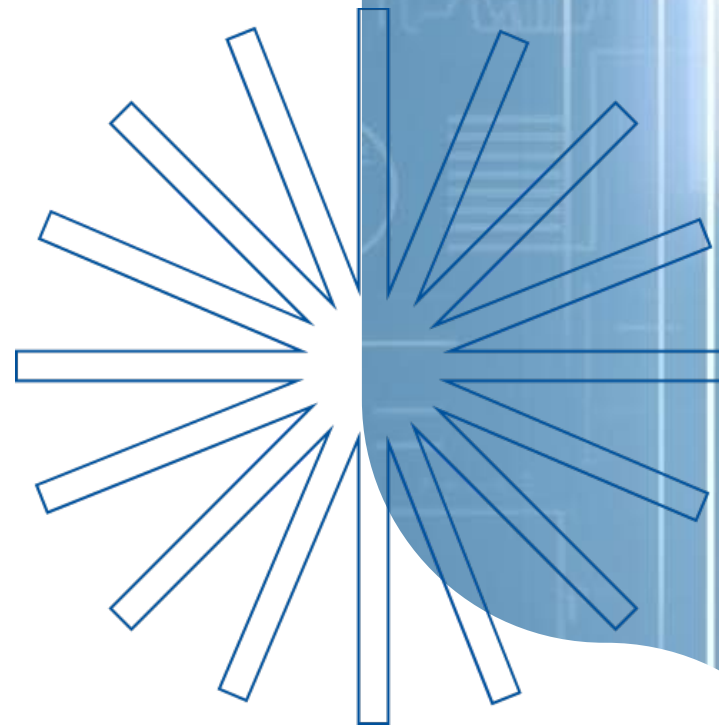
PRESENTED BY
Clarence CHAU

DATE
24 October 2025



Why We Are Here?

- The digitalisation of Hong Kong's healthcare system offers immense **opportunities** but exposes critical **cybersecurity vulnerabilities**.
- Cybersecurity not just as a technical challenge but as a critical enabler of trust, safety of healthcare industry. **Collaboration** between stakeholders is the foundation of **immunity** and **resilience**.



Development Milestones of eHealth

醫健通
ehealth

2009 - 2016

Stage 1 Development

- (2015) eHRSS Ordinance (2015)
- (2016) eHR sharing platform (2016)



2017 - 2022

Stage 2 Development

- eHealth App (2021)
- Sharing of radiological images and CM information

醫健通+
eHealth

香港特別行政區政府 HKSARGOV'T

2024 - 2029

醫健通+
eHealth+

- **Comprehensive healthcare information infrastructure** for data sharing, service support and care journey management

Integrated Eco-system Supported by eHealth+



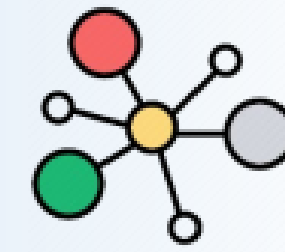
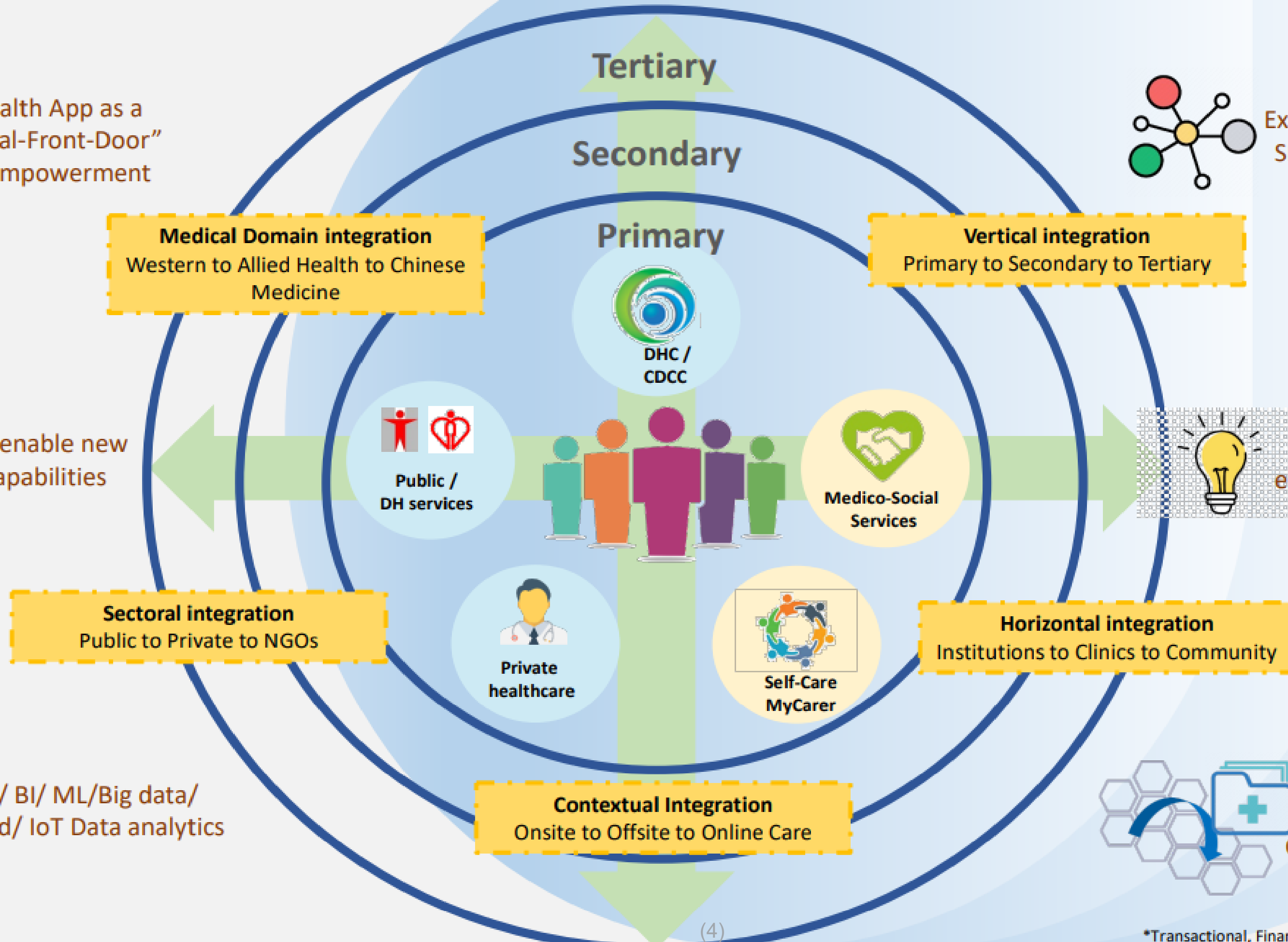
eHealth App as a
“Digital-Front-Door”
for empowerment



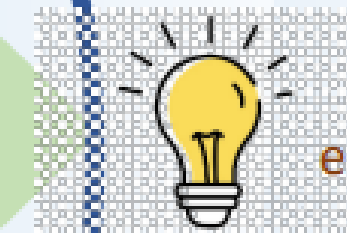
Telehealth enable new
service capabilities



AI/ BI/ ML/Big data/
Cloud/ IoT Data analytics



Extend PPP / DHC/ CDCC /
SP/ Primary Care service
and sharing scope



eHealth as central data hub*
for research and analytics
Data Linkage with HCPs,
Insurance and B&D



Cross border data access
and download

eHealth Digitalisation Impact

Overview of key statistics in
Hong Kong's healthcare
transformation

6,900 +

Healthcare Service
Location

6 million +

Healthcare Recipient
Registration

3.8 million +

eHealth App
Download

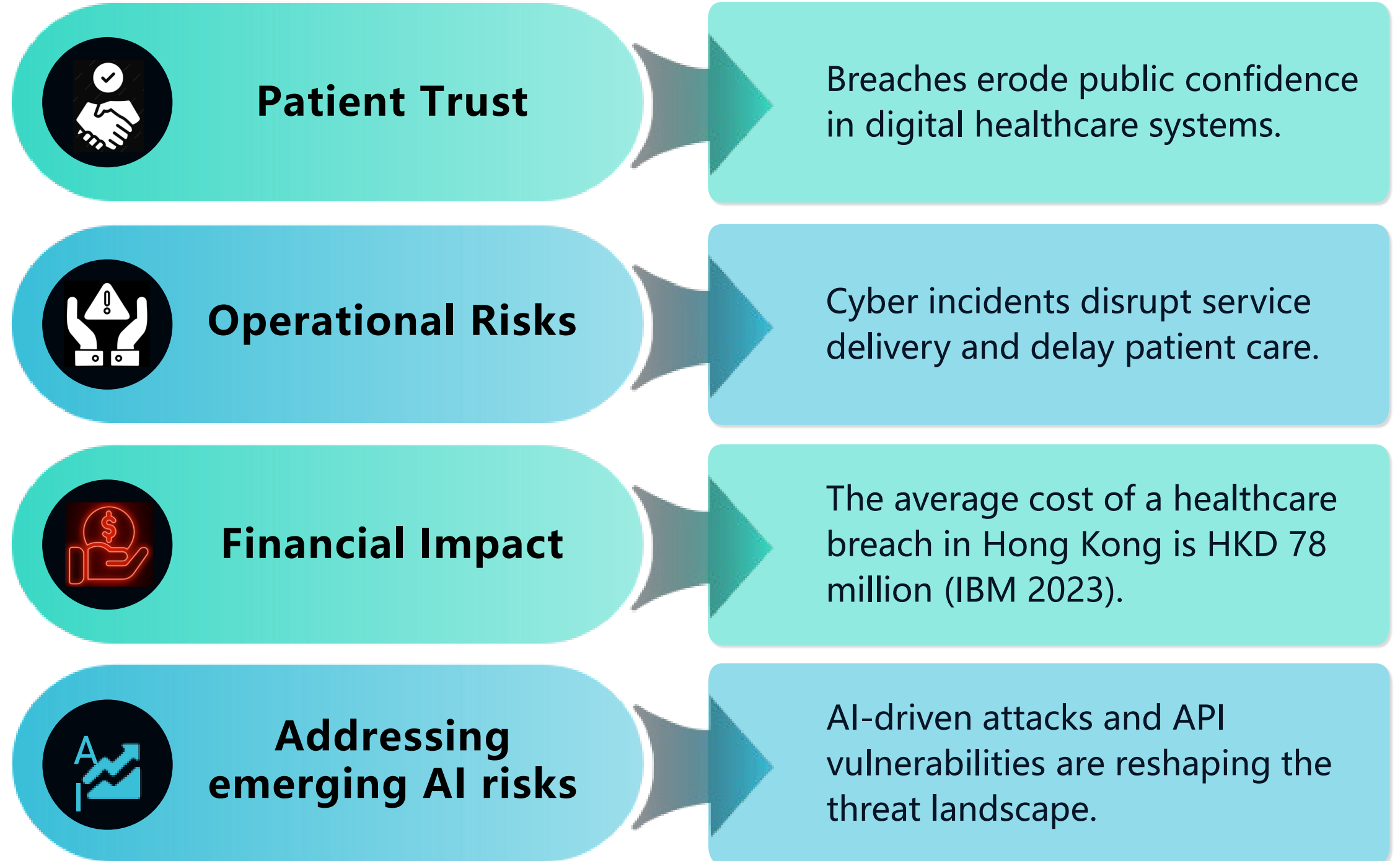
275 000 +

eHealth Record
Assess Per Month

Cybersecurity in eHealth is not just about protecting systems — it's about safeguarding patient trust, ensuring uninterrupted care, and mitigating financial and reputational risks.



Building Digital Immunity in eHealth: Why?



Cybersecurity Foundations for eHealth+

eHealth+ Priorities

Expand connectivity, enhance data sharing, support cross-boundary data sharing

Support primary health and cross-sectoral healthcare services

Enrich ehealth app services and linkage with HCPs to position eHealth App as “frontdoor” of all healthcare services

Encourage healthcare eco-system development & integration

1



Cybersecurity Risks

↑ Exposure
↑ Connectivity
↑ Data sharing
↑ Users
↑ Integration pts
↑ eHealth footprint

↑
Risks

2



Cybersecurity Principles

Defense in Depth
Security by Design
Privacy by default
Zero Trust / least Privilege
Continuous monitoring
Fast incident response
People first (Awareness)

3



Cybersecurity Challenges in Hong Kong eHealth EcoSystem

Supply Chain Risk

Many organisations rely on vendors for IT operations, but these vendors can become the weakest cybersecurity link. Without regular reviews, they may expose sensitive data to risks.

60%

data breaches in HK related to 3rd party service providers in 2023

Phishing / Ransomware Trends

The rise of ransomware in healthcare globally shows its potential to disrupt Hong Kong healthcare operations

66%

of healthcare organisations worldwide reported ransomware attacks in 2022

Insufficient IT Training

Many healthcare staff remain unprepared to handle cyber threats.

40%

HK Org conduct regular training

Security Threats in
the Intreality Fiallsus:
Mealitive at-Healthcane
essential snencition

Emerging Threats

API and IoT Security Gaps on medical devices

Weak API and IoT security measures expose critical integration points and connected devices to vulnerabilities.

50%

healthcare data breaches globally in 2022 were due to insecure APIs and poor database configuration (IBM 2022)

Cloud-based EMR Risks

Cloud-based EMR solutions raise concerns over data sovereignty, vendor lock-in, and insufficient security safeguards.

43%

of cyberattacks on healthcare globally in 2022 targeted cloud-based applications. (Cloud Security Alliance Report 2022)

AI-Driven Risks with Generative AI

Generative AI poses risks such as data privacy breaches, output inaccuracies, regulatory non-compliance, and exploitation by malicious actors.

63%

of organisations worldwide report concerns about AI-related cybersecurity risks (Gartner 2023)

Mitigating Supply Chain Risks

60% data breaches in HK related to 3rd party service providers in 2023 (PCPD)

42% HK IT systems using APIs without adequate security measure in 2022 (HKCERT)

Why It Matters?

- Potential vulnerabilities arise when organisations rely on **third-party vendors or service providers**, whose security weaknesses—such as embedded software or hardware vulnerabilities, or misconfigurations in firewalls, APIs, and databases—can compromise the entire system.

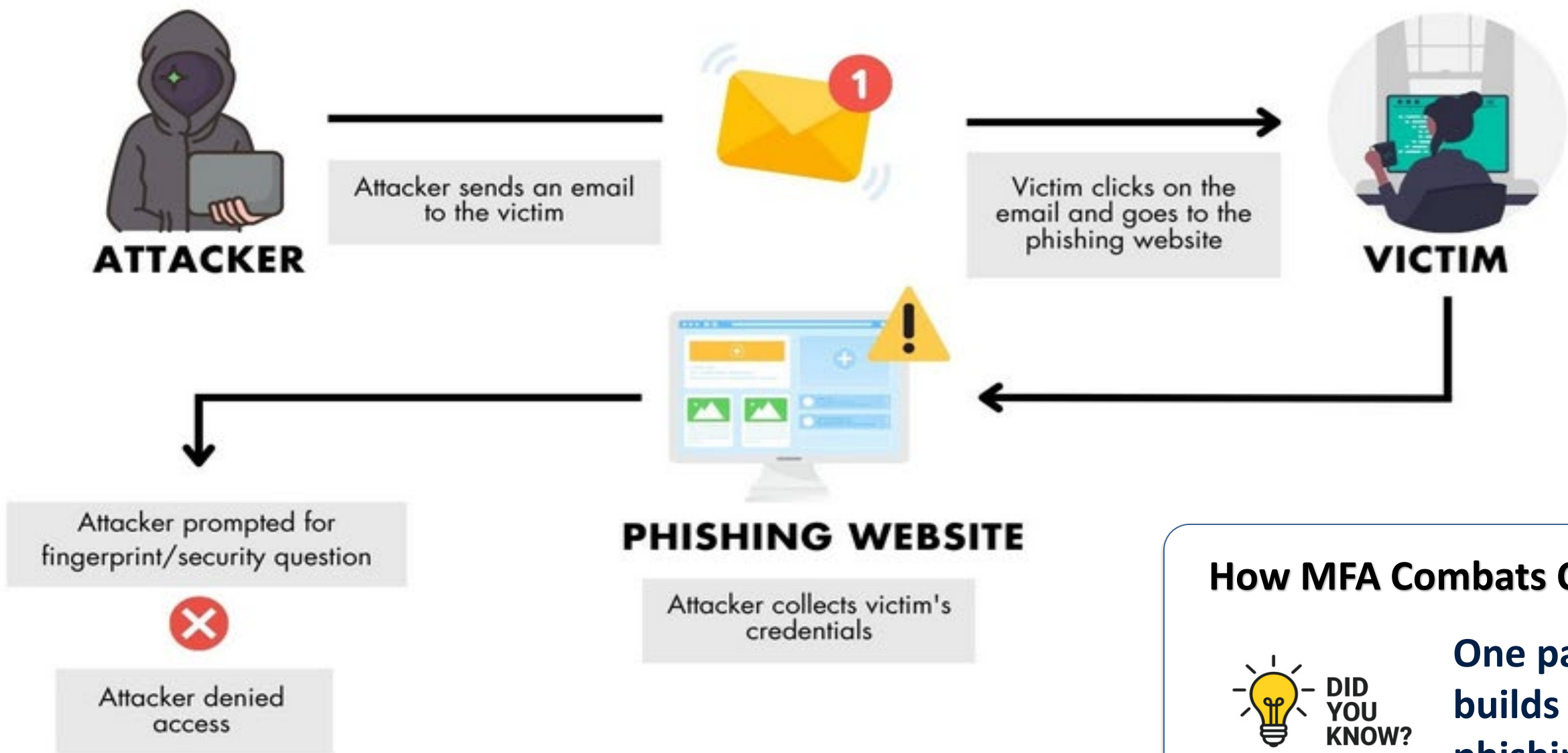
Mitigation Strategies

- Conduct third-party risk assessments (SRAA) regularly.
- Implement a zero-trust model for vendor access.
- Require vendors to adhere to strict security standards.
- Establish collaborative incident response plans.

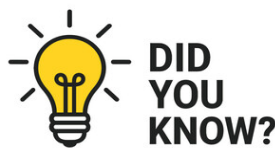


Phishing, Spear Phishing and Whaling

66% of healthcare organisations worldwide reported ransomware attacks in 2022 (Sophos)



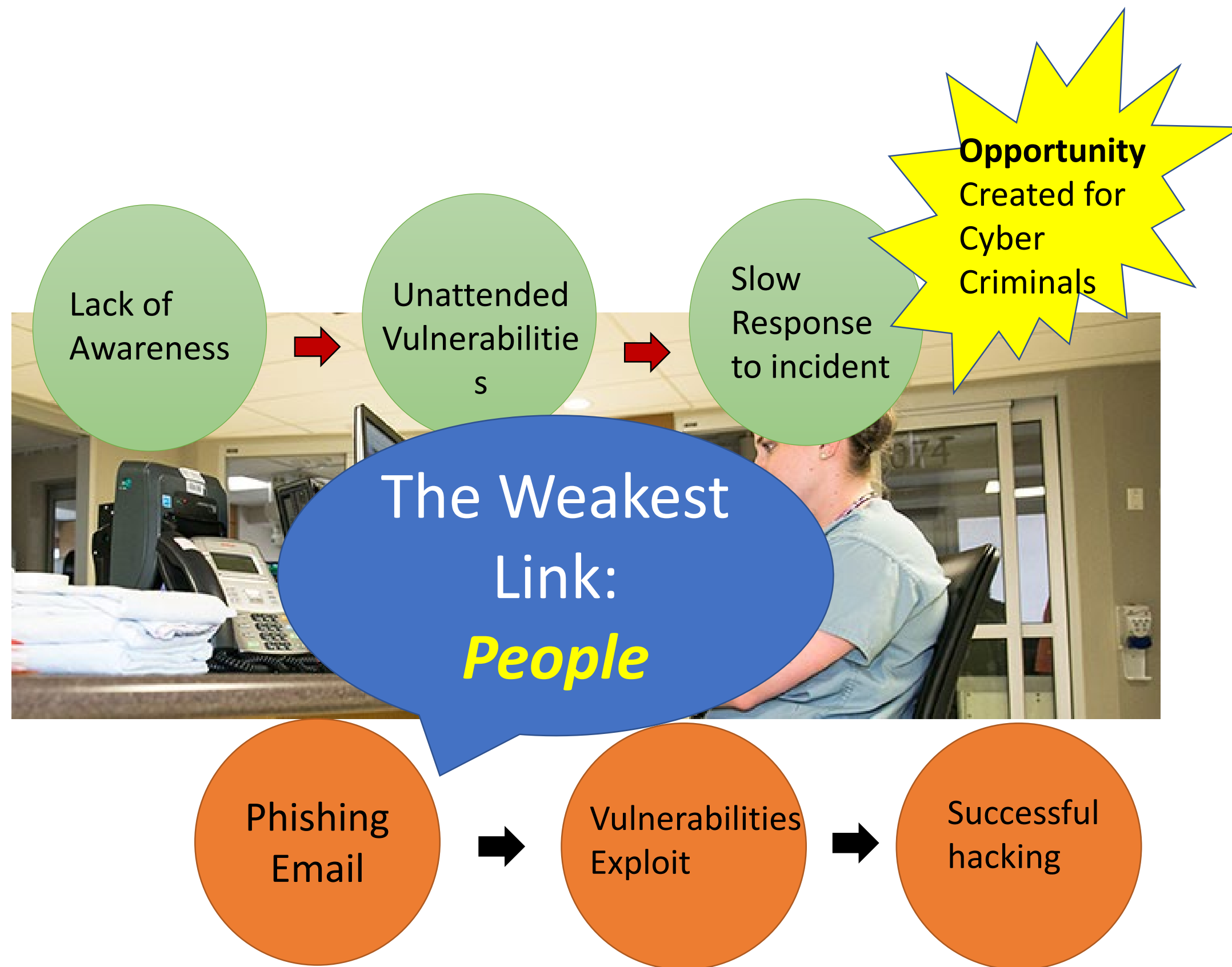
How MFA Combats Common Attacks of Phishing?



One password can be stolen, but MFA builds a fortress — protecting against phishing, spear phishing, and beyond.

Similarity of these incidents

People are the weakest link; vigilance defeats phishing every time.



API and IoT Security in eHealth

IoT devices, such as health stations and wearable devices, capture personal health data and upload it to eHealth platforms.

Why It Matters?

- Weak authentication exposes sensitive health data.
- Unsecured transmission allows data interception or tampering.
- Outdated firmware increases device vulnerabilities.
- Unencrypted or poorly secured data, whether locally or in the cloud, can be extracted or leaked.

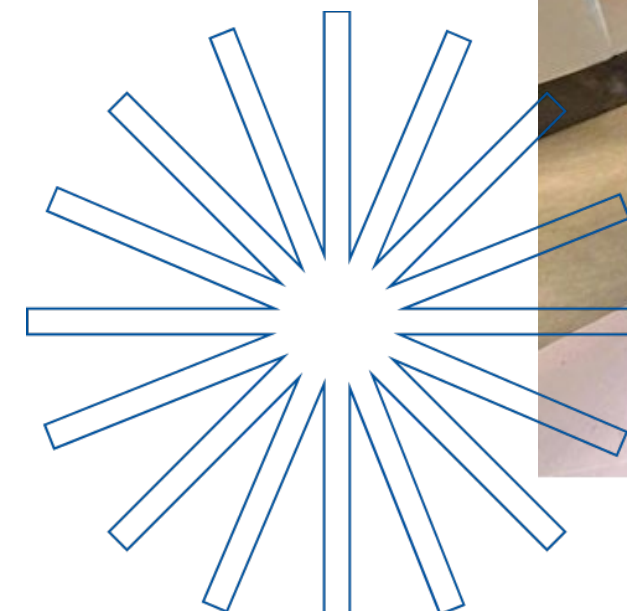
Mitigation Strategies

- Encrypt all data transmissions.
- Use strong authentication controls.
- Ensure regular device updates.
- Assess device security before integration.



15%

IoT cyberattacks globally target healthcare (Frost & Sullivan 2022)



Cloud-based EMR Risks

Cloud SaaS Risks

Cloud-based solutions (e.g., SaaS platforms) are widely adopted but present unique challenges:

1. Data Breaches: Shared cloud environments increase data exposure risks.
2. Operational Disruptions: Platform downtime impacts service continuity.
3. Vendor Lock-In: Migration to alternative solutions can be complicated.

Best Practices for Engaging Cloud Vendors

- Ensure clear SLA for security, uptime, and data protection.
- Maintain regular backups of clinical records and ensure migration options to alternative solutions are viable.
- Regularly review vendors' cloud security certifications.
- Verify the vendor's ability to notify and respond promptly to breaches.



AI-Driven Risks with Generative AI



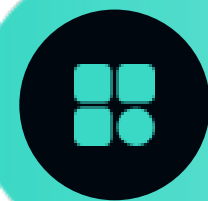
Sensitive Data Leaks

- Inputting patient data into generative AI tools can inadvertently expose sensitive information.



Prompt Exploitation

- Poorly constructed prompts or misuse of AI tools may lead to unintended data sharing or malicious manipulation.



Reliance on External AI Models

- Public AI platforms may lack sufficient security controls for handling healthcare data.

Case Study

AI Transcription Leak (2023): A generative AI tool used for medical transcription exposed patient records due to unencrypted prompts

Medical Transcription Provider Hacked, Compromising Data for Nearly 9M People



Transcription is in the news — though in this case, “bad press” is worse than “no press.” Medical transcription provider Perry Johnson & Associates disclosed in a filing with the US Department of Health and Human Services a massive security breach that affected more than 8.95m individuals, [TechCrunch reported](#) November 15, 2023.

The cyberattack — which TechCrunch described as “one of the worst medical-related data breaches in recent times” — began as early as March 2023. PJ&A began notifying patients whose information was compromised on October 31, 2023.

The stolen data included patient names and dates of birth, addresses, and

some social security numbers, all of which could be used in identity theft. Medical records, admission diagnoses, and dates and times of services were also among the sensitive information.

Of the nearly 9m patients whose information was breached, 3.89m were patients of the Northwell Health system. Notably, this the second breach of Northwell Health patient data in 2023, after another transcription provider, Nuance Communications, fell victim to a mass hack.

PJ&A explained in a [statement](#) on its website that “an unauthorized party” accessed and acquired copies of certain files from March 27-May 2, 2023.

The company noted that “we have no evidence that individuals’ information has been misused for the purpose of committing fraud or identity theft,” but established a “dedicated toll-free call center” for affected individuals to discuss concerns about the breach.

- A generative AI tool used for medical transcription.
- Unencrypted Prompts exposed sensitive patient data.
- Thousands of health records compromised.
- Unsecured AI processing exposed PII.
- Potential triggered regulatory violations.



Establish Internal Guideline for Staff

Best Practice on Using GenAI

Smart Tip 1: Do NOT rely on GenAI as an authoritative source of knowledge
核實結果 - 不要依賴 GenAI 作為權威消息來源

Smart Tip 2: Do NOT submit sensitive or personally identifiable information
保護私隱 - 避免提交敏感或者個人身份資料

Smart Tip 3: Be responsible for your co-created output with GenAI
用戶負責 - 確保你和 GenAI 創建的內容是準確和可靠的

Generative Artificial Intelligence (AI) tools and platforms allow users to generate all sorts of novel contents, such as audio, text, code, video, image and other data. This includes AI chatbots such as "ChatGPT" which are programmes based on a large language model with the ability to generate natural language text based on a given input. In light of the growing popularity of AI chatbots, the Office of the Privacy Commissioner for Personal Data provides the following tips for users of AI chatbots to protect their personal data privacy and to use them safely and responsibly:

Protecting Personal Data Privacy



Before Registration / Use:

- 1 Read the Privacy Policy, the Terms of Use and other relevant data handling policies of AI chatbots and any third-party platform used to access the chatbots to understand how personal data would be collected, stored, used, and shared.
- 2 Beware of fake Apps and phishing websites posing as known AI chatbots: access AI chatbots only through official channels and only install Apps from the official Apps stores.
- 3 Adjust the settings to opt-out of sharing chat history (if available) to avoid conversations being saved and used for AI model training.



When Interacting with AI Chatbots:

- 4 Refrain from sharing your own personal data and others' personal data as conversation history may be stored and used for AI model. Consider using a nickname or pseudonym instead of providing AI chatbots with real name.
- 5 If necessary, submit a correction or removal request to correct or remove any inaccurate personal data generated by AI chatbots.
- 6 Guard against cybersecurity threats: use secure network connection to connect to AI chatbots and keep device system and software up-to-date.
- 7 Delete outdated conversations from chat history. Delete unused AI chatbots accounts to reduce the risk of data leakage.



Safe and Responsible Use of AI Chatbots

- 8 Be cautious about using the information provided by AI chatbots: check the accuracy of such information through other sources as information generated by AI chatbots may be misleading, false, biased or discriminatory, owing to insufficient and/or inaccurate training data. Also beware of intellectual property rights issues and avoid using the information in breach of such rights.
- 9 Refrain from sharing confidential information and files; organisations should promulgate clear internal policies and guidance for using AI chatbots.
- 10 Teachers / parents should provide guidance to students when they are interacting with AI chatbots: AI chatbots may set a minimum age for users and require students under a specified age to obtain parent or guardian's permission before use. Teachers / parents may prompt AI chatbots to provide age-appropriate responses to reduce the chance of children being exposed to inappropriate content.

Take Reference to PCPD Resources about AI Security

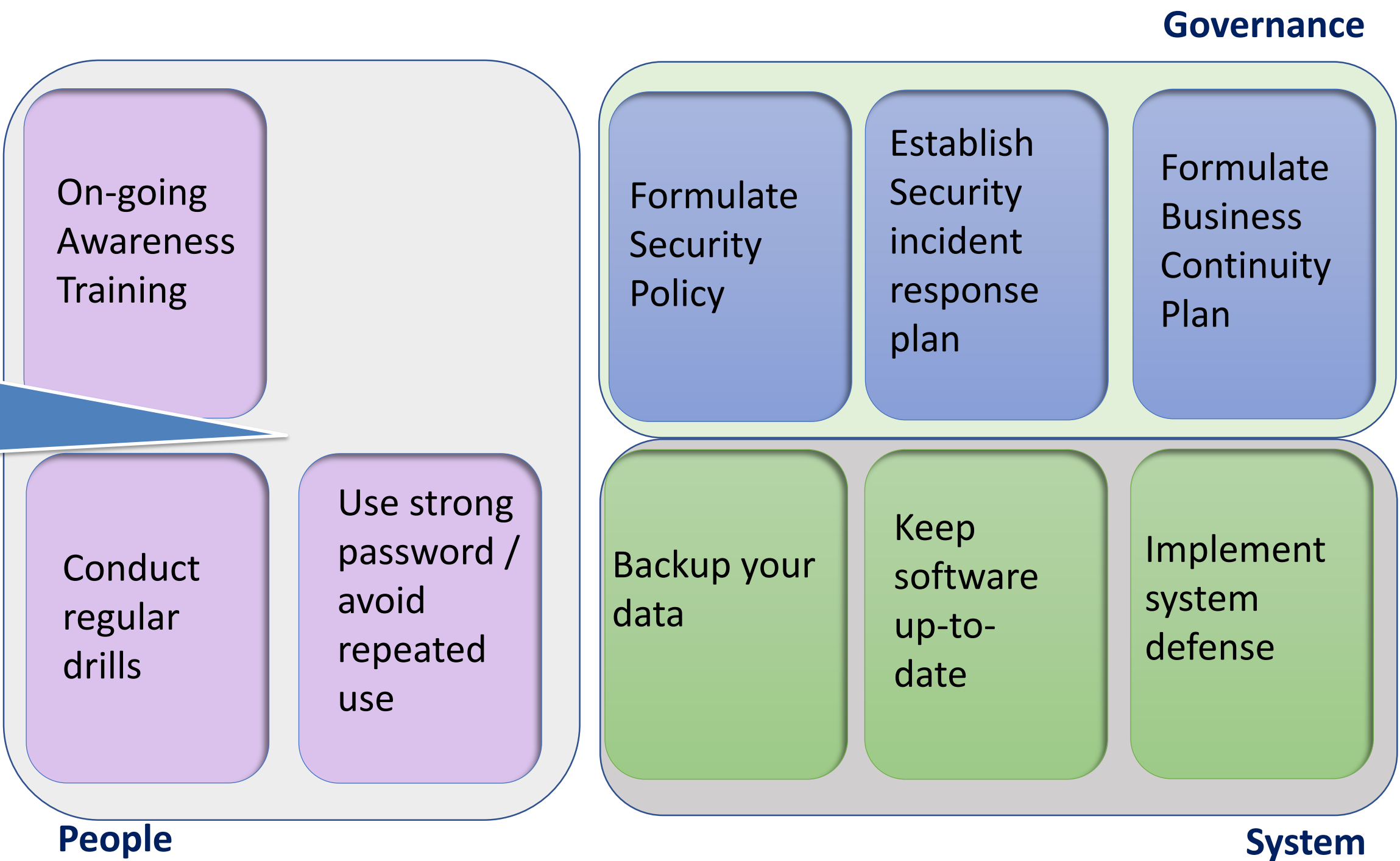
URL: https://www.pcpd.org.hk/english/artificial_intelligence/index.html



Build Cybersecurity Resilience

Prepare, Protect, Persevere: Resilience Against Cyber Threats!

The Weakest
Link:
People



eHealth App

A Trusted Source for Secure Healthcare Integration

Authentication Made Easy

The eHealth App provides seamless authentication with HA Go and other medical group applications, similar to China's WeChat, ensuring efficient booking and access to healthcare services.

Enhanced Security

eHealth is leveraging iAM Smart technology to strengthen security protocols, ensuring that user data remains confidential and protected from unauthorized access during interactions.

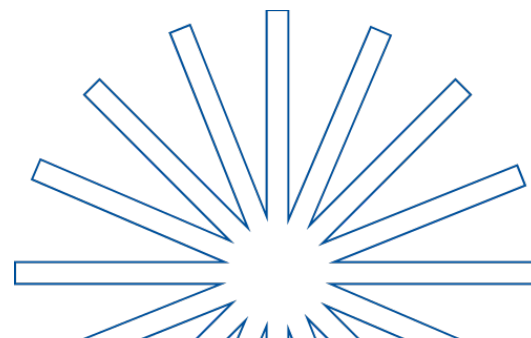


Secure Data Transfer

The eHealth App enables secure transfer of Cross-border Health Record data and radiology imaging, allowing for safe sharing of critical medical information between healthcare professionals and patients.

Future Capabilities

In the future, the eHealth App can validate electronic Advanced Medical Directives (eAMD), e-Sick leave certificates, and provide secure access to partner services (e.g. eBooking), enhancing its utility for citizens and professionals.



Financial Commitment to Cyber Security

INVESTMENT COMMITMENT

eHealth+ will allocate 10% of total costs to strengthen overall cybersecurity for eHealth and the wider ecosystem.

ALLOCATION PRIORITIES

1. Technology acquisition (AI, quantum encryption, API security).
2. Staff training and awareness programmes.
3. Incident response planning and drills.

CYBERSECURITY



Security Policies

Diagrams of policies and procedures for the organization, including the use of secure communication channels, the use of secure data storage, and the use of secure data transmission.



Incident Response Plan

Diagram illustrating the incident response process, including the identification of the incident, the assessment of the impact, the containment of the incident, the eradication of the incident, and the recovery of the system.



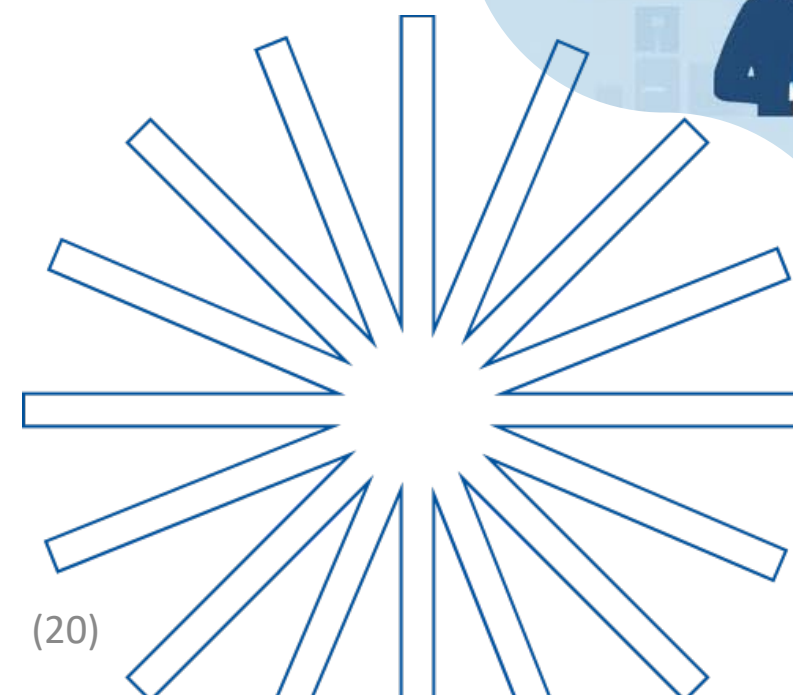
Incident Response Plan

Diagram illustrating the incident response process, including the identification of the incident, the assessment of the impact, the containment of the incident, the eradication of the incident, and the recovery of the system.



Incident Response Plan

Diagram illustrating the incident response process, including the identification of the incident, the assessment of the impact, the containment of the incident, the eradication of the incident, and the recovery of the system.





Joining Forces for a Secure Future

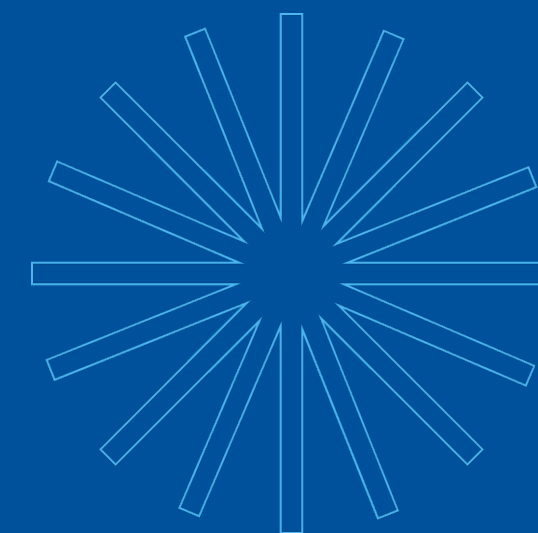
RECAP

Cybersecurity is vital to eHealth and all partners in healthcare industry, any incidents may affect **patient trust**, **operational continuity**, and **financial stability**.

Collaboration and **investment** are key to a resilient healthcare ecosystem

Together, we can secure Hong Kong's healthcare future and protect patient trust in the digital age.

THANK YOU



醫健通+
eHealth
香港特別行政區政府 HKSARGOVT