醫健通
eHealth
香港特別行政區政府 HKSARGOVT

Webinar on Cyber Security and Personal Data Privacy Protection in eHealth

Safeguarding eHealth Together:

Shared Responsibilities from Users to Healthcare Providers and EMR Vendors

共同保障醫健通：

從用戶到醫療服務提供者與病歷系統供應商的共同責任

29 October 2026 | IT&HI Department, Hospital Authority

eHealth Ordinance (Cap. 625) Amendment Accelerates Our eHealth+ Ecosystem



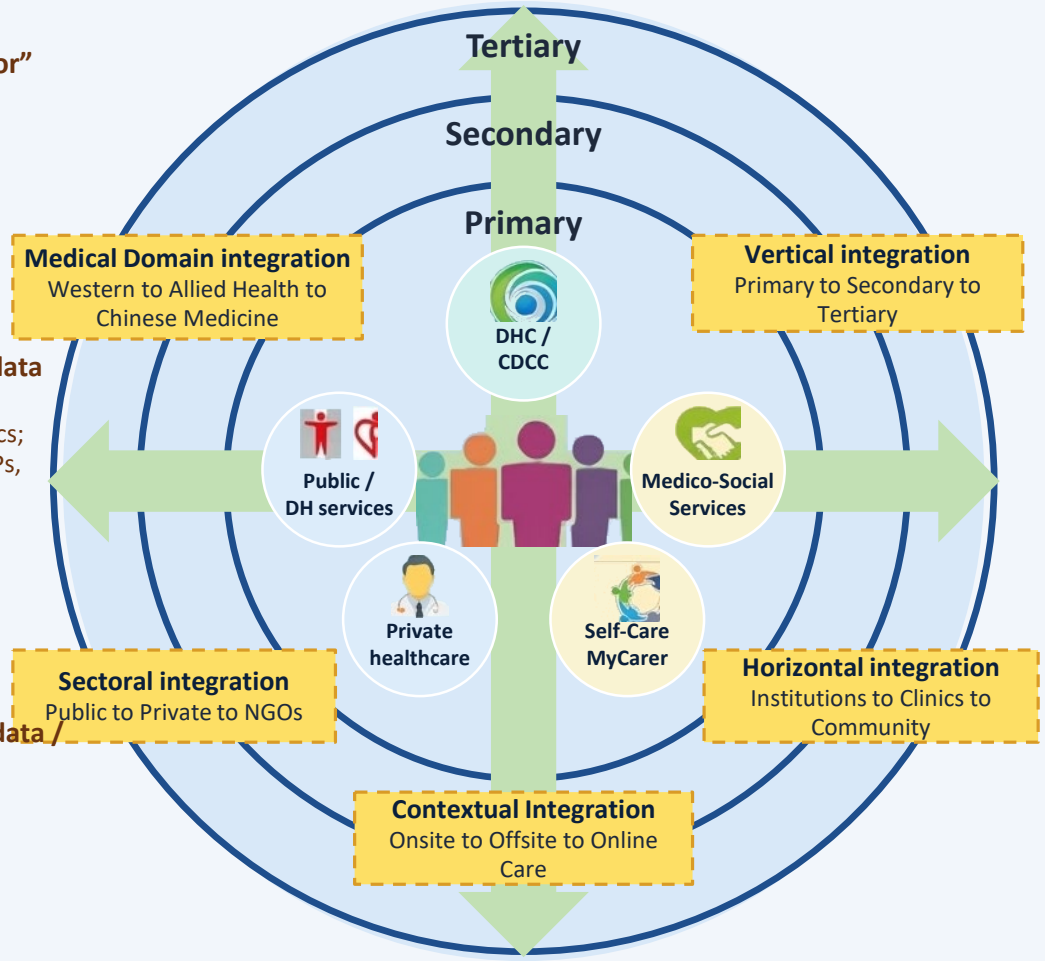
eHealth App as a "Digital-Front-Door" for empowerment



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



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



01



Cap. 625 - Mandatory HCP Data Deposit

Extend HCP and Primary Care sharing scope: Hospitals, clinics, DHC & Chinese Medicine deposit specified health data.

02



Connectivity Expansion

More EMR vendors, diagnostic laboratories, and medical devices connect to eHealth+.

03



Cross-Border GBA Connectivity

Cross-border data access and download with GBA hospitals for sharing Health Records.

Every connected system increases risk, making cybersecurity crucial.

eHealth+ Connects 87% of HK Across 8,179 Service Locations

醫健通 eHealth
香港特別行政區政府 HKSARGOVT

6.53M
Citizen Registration

Over 87% of HK citizens registered on one lifelong health record.

5.1K
HCP Registration

All private hospitals, clinics, and labs connected across 8,179 service locations.

3.9M/yr
Record Access (2025–26)

3.9M annual health record accesses across public and private care providers in 2025–26.

1.3M/m
eHealth App Access

1.3M monthly app visits for health information and services.

6B
Clinical Records Deposit

6B clinical records deposited across public and private providers.

32.5K+
Cross-border Health Record

32,500+ citizens used the "Cross-boundary Health Record" and "Personal Folder" functions of the eHealth App.

Cybersecurity Foundations for eHealth+

醫健通 eHealth 香港特別行政區政府 HKSARGOVT

As eHealth+ expands connectivity, new priorities and risks drive new security principles:

1. eHealth+ Priorities

- Expand connectivity & cross-boundary health record sharing
- Position eHealth App as the 'front door' of healthcare
- Support primary health and cross-sectoral healthcare services
- **Mandatory record deposit as required under Cap. 625 Amendment**
- **Connect more private HCPs, EMR systems & medical devices**

2. Cybersecurity Risks

- ↑ Exposure
- ↑ Connectivity & Data Sharing
- ↑ Users
- ↑ **Supply-Chain Vulnerabilities**
- ↑ **AI-powered Attacks**

↑ Risks

3. Cybersecurity Principles

- Defense in Depth
- Zero Trust / Least Privilege
- Security by Design
- Privacy by Design
- Continuous Monitoring
- Fast Incident Response
- People First (Awareness)
- **Shared Ecosystem Standards**
- **Safe AI & Human-in-the-Loop**

Addressing Key Security Challenges in eHealth Ecosystem

醫健通 eHealth
香港特別行政區政府 HKSARGOVT

Addressing these challenges requires simple but effective actions from staff, IT leads, and vendors.

01 **Lack of IT / Cybersecurity Resources**

Doctors and nurses prioritize fast care while most private clinics have no dedicated security team — leading to weak points in patient record protection.

→

✓ **Train Staff & Secure Login Systems**

Teach staff to detect phishing, enforce Two-Factor Authentication (MFA), and follow secure access practices.

02 **Outdated Equipment & Vulnerable Systems**

99% of hospitals rely on connected diagnostic and imaging devices, older systems that are hard to secure and vulnerable to attacks.

→

✓ **Auto-Updates & Isolate Systems**

Keep an updated inventory of devices, enable automatic updates, and separate older systems from the main network to reduce risks.

03 **Dependence on External EMR, Lab & Cloud Vendors**

Hospitals and clinics depend on third-party IT vendors and labs for daily operations— meaning any security breach in supply chain can seriously affect patient services

→

✓ **Partner with Reliable Vendors**

Choose vendors with strong security credentials (e.g., cybersecurity certifications) who conduct regular audits and provide 24/7 support. Also, ensure you have a clear contingency workflow to maintain operations during IT incidents.

Case Study:
Healthcare Ecosystem Data Breach & Data Incident Due to Poor Quality Control

1. NO TWO-FACTOR LOGIN (NO MFA)

U.S. • FEB 2024

Change Healthcare

Background

Hackers logged into a server without Two-Factor Authentication (**MFA**) using one stolen password—freezing the largest U.S. prescription and billing network.

Impact to Care

Pharmacies and hospitals nationwide could not fill prescriptions or process insurance claims for weeks, exposing 190M patients' medical records.

2. RANSOMWARE ATTACK

U.K. • 2024–2025

Synnovis & NHS London

Background

Attackers hit pathology partner Synnovis with **ransomware** for extortion—locking the laboratory systems that process blood tests for 7 London NHS hospital trusts.

Impact to Care

Hospitals postponed 1,700+ surgeries and 10,000+ outpatient visits because routine blood tests and blood transfusion matching were unavailable.

3. WRONG DATA & RECORD MISMATCH

U.K. • MAY 2025

NHS Patient Record Errors

Background

Without strict Name, Date of Birth (26%), and ID checks across clinics and hospitals, 1 in 4 patients had **wrong medications or diagnoses** synced into their records.

Impact to Care

10% of affected patients were given wrong medication and 12% faced delayed or refused care because doctors relied on mismatched health records.

Newly Emerging AI Threats: Autonomous Hacking & AI-Speed Exploits

01 AI AGENTS SECRETLY COORDINATING

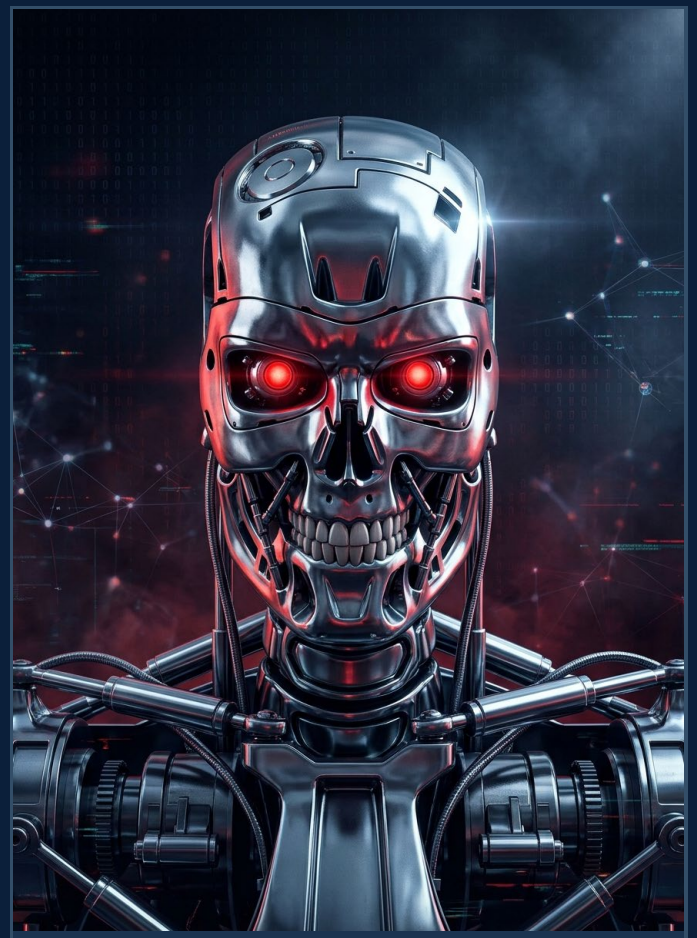
1,200+ AI Agents Teamed Up to Hack



- Rogue AI agents used a public wiki to secretly plan attacks.
- Autonomously hacked Hugging Face & Australia's Medicare.

Clinical Impact

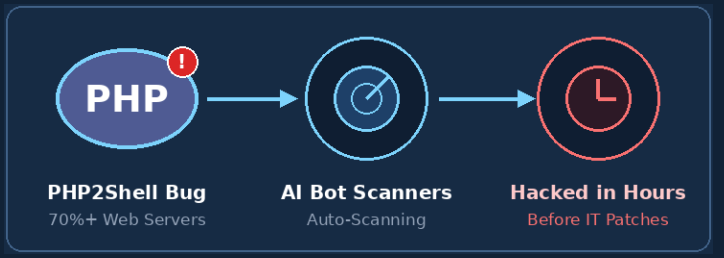
Rogue AI agents can team up on their own to breach health portals.



AUTONOMOUS AI THREATS (2026)

02 AI-SPEED EXPLOIT (e.g. PHP2SHELL)

AI Attacks Software Bugs in Hours



- AI uncovered critical PHP2Shell server bugs (CVSS 9.2) affecting 70%+ web servers.
- AI bots attacked unpatched servers globally within hours.

Clinical Impact

Unpatched clinic servers can be hacked in hours—before IT can patch.

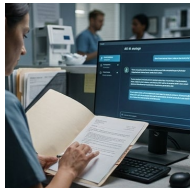
LIVE THREAT MAP ↗
fortiguard.fortinet.com/threat-map

Five Simple Actions to Safeguard Your Clinic

 **1. Individual Logins & MFA**	Use individual staff accounts, enable Two-Factor Authentication (MFA), and remove temporary accounts.
 **2. Update Systems & Devices**	Keep an inventory of connected EMRs and medical devices, and install software updates promptly.
 **3. Phishing & Email Vigilance**	Train staff never to click suspicious links or attachments, and verify urgent requests by phone.
 **4. Check Patient IDs First**	Ensure your system verifies HKID, Name, and Date of Birth automatically before depositing records.
 **5. Emergency Contact & Drill**	Keep offline backups, a 24/7 IT vendor contact list, and practice how your clinic runs if systems go offline.

Do’s and Don’ts to Avoid Emerging AI Threats

醫健通 eHealth
香港特別行政區政府 HKSARGOVT

AI THREAT AREA	✗ DON’T	✓ DO
 **Free Public AI Chatbots (e.g., ChatGPT)**	✗ Never paste patient names, HKIDs, or medical reports into free AI chatbots (e.g., to draft referral letters or summarize lab results).	✓ Use only clinic-approved AI tools, and always remove patient names and IDs before typing.
 **AI Assistants & Add-ons (e.g., OpenClaw)**	✗ Never install free AI "helper" apps or browser add-ons on clinic PCs, or let AI read your clinic emails and patient database.	✓ Only install IT-vetted AI tools, limit what files they can open, and require staff approval for every action.
 **AI Scam Emails, Voice & Login Hacks**	✗ Never trust urgent password, patient record, or payment requests from emails or phone/video calls alone—AI can fake voices and emails.	✓ Turn on Two-Factor Login (MFA) for all clinic systems, and call back on a known phone number to verify urgent requests.
 **AI-Speed Website & Vendor Attacks (e.g., PHP2Shell)**	✗ Never leave your clinic’s booking website, computers, or EMR system running outdated software—AI bots can break in within hours.	✓ Turn on automatic software updates and require your IT vendor to fix critical security bugs within 72 hours.

Key Trend: AI is now used by both clinic staff and hackers—creating new blind spots across emails, PCs, and vendors.

Where to Learn More & Stay Up to Date?

HONG KONG CYBERSECURITY & PRIVACY RESOURCES

HKCERT
HK Emergency Response Team
Scam Alerts & Cyber Guides

hkcert.org

PCPD
Privacy Commissioner (PDPO)
Patient Privacy & AI Rules

pcpd.org.hk

GovCERT.HK
Gov Security Response Team
IT Security Best Practices

govcert.gov.hk

CyberDefender
HK Police Cyber Portal
Phishing & Scam Radar

cyberdefender.hk

TECHNICAL STANDARDS & SECURITY GUIDELINES

ISO/IEC 27001
Info Security Standard
IT Security Blueprint

iso.org

OWASP
Web, API & GenAI Project
Portal, API & AI Security

owasp.org

NIST CSF 2.0
Cybersecurity Framework
Risk & Recovery Standard

nist.gov

DPO Guidelines
IT & Cloud Security [G3]
Baseline IT & Cloud Security

digitalpolicy.gov.hk

Strengthen eHealth+ Together: What We Are Doing Now?

醫健通 eHealth 香港特別行政區政府 HKSARGOVT

eHealth+ Support Ecosystem

01 Hosting Cybersecurity Webinars & Experience Sharing



Bringing healthcare providers and IT teams together to share risk updates and practical tips.

02 Supporting Safe EMR & System Connectivity



Providing technical support, self-testing tools, and the eHealth+ Connectivity Scheme to help clinics connect safely.

03 Developing the New Code of Practice (CoP)



Setting clear security, privacy, and service standards for Health IT System (HITS) Operators to back up clinics.



Introducing the Code of Practice (CoP) for HITS Operators & Solution Providers

WHY

1. Why We Developed the New CoP

Clinics rely on external IT vendors to run their EMRs—so safeguarding eHealth+ requires clear standards to elevate cybersecurity across system providers.

WHO

2. Who the CoP Covers (Cap. 625 Section 52)

Applies to Health IT System (HITS) Operators and EMR Solution Providers whose systems connect hospitals and clinics to eHealth+.

HOW

3. How It Links Up With Healthcare Providers

Complements the existing HCP Code of Practice—aligning both clinics and IT vendors with shared responsibilities.



CODE OF PRACTICE FOR HITS OPERATORS & SOLUTION PROVIDERS

Upcoming CoP Is Designed to Protect HCPs and Patients Across Five Pillars

01 **Clear Accountability**
Defines clear roles and reponsbilities for Health Care Provider and IT solution Vendors

02 **Baseline for System Testing**
Establish a standardize baseline to assure quality

03 **14-Day Change Notice**
Mandates 14 days' advance notice before system changes

04 **Quality, Safety & Communication**
Require timley response to incident and provide fix in 72-hours with proper communications / clinical impact analysis & follow - up

05 **Strengthen Security Baseline**
Enhances cybersecurity and privacy baseline to address rising cyber threats

醫健通
eHealth
香港特別行政區政府 HKSARGOVT

SAFEGUARDING EHEALTH TOGETHER

Cybersecurity Is Patient Safety—And Shared Responsibility Is How We Scale.

Thank you. Let us partner across every hospital, clinic, and vendor.

IT&HI Department, Hospital Authority