

# 當醫療器材被駭：從真實事故看醫療資安的重要性

*When Medical Devices Get Hacked: Lessons from Real Incidents and the Need for Secure Medical Software*

醫療資安研討會



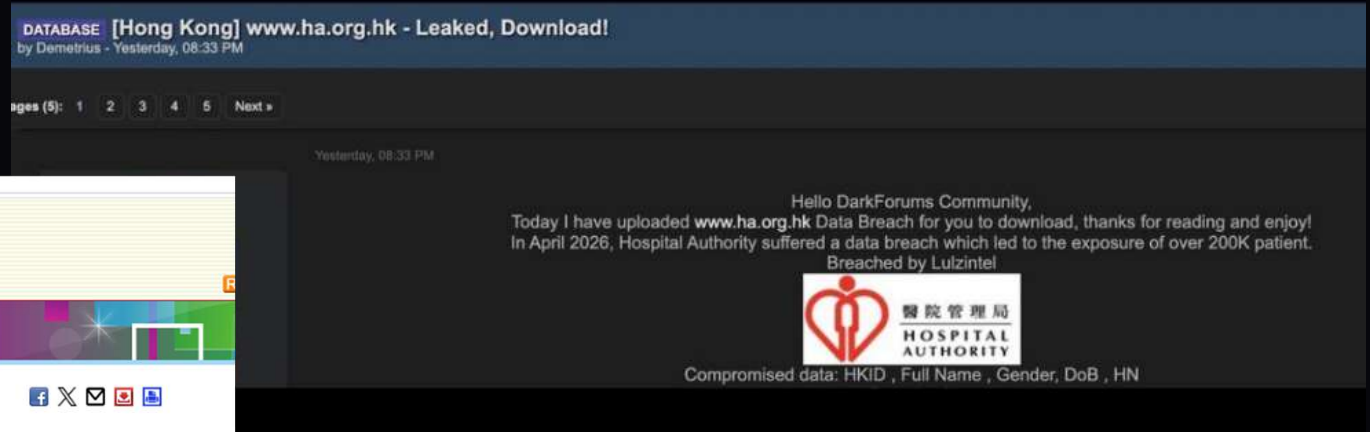
香港品質學會  
Hong Kong Society for Quality



# About the speaker

- **Norton Yuen, PhD**
  - CEH / CEH Practical / CEH Master
  - ISO 17025 Technical Assessor / Former Senior Lecturer / TIC industry practitioner
- Laboratory Director, The One Testing Technology Company Limited
- 20+ years in testing, certification, and laboratory operations
- Focus areas: cybersecurity testing, laboratory systems, and quality management

# 最近新聞



香港特別行政區政府  
新聞公報

GovHK 香港政府一站通 简体版 English

醫院管理局懷疑有病人資料於第三方平台洩漏的聲明

醫院管理局懷疑有病人資料於第三方平台洩漏的聲明  
\*\*\*\*\*

下稿代醫院管理局發出：

醫院管理局（醫管局）發言人今日（四月四日）就懷疑有病人資料於第三方平台洩漏事件作出以下聲明：

醫管局的恆常監察系統於昨日（四月三日）凌晨二時許發現一宗懷疑未經授權將病人資料取走並於第三方平台洩漏的個案，隨即於早上報警及通報個人資料私隱專員公署，醫管局會全面配合警方調查及行動。

事件涉及的56 000多名病人來自九龍東醫院聯網，外洩資料包含病人姓名、性別、身份證號碼、醫院檔案號碼及手術內容等資料。

醫管局向受影響病人致歉，並將採取一切可行措施，務求將對病人影響減至最低。醫管局會盡快透過「HA Go」應用程式、郵寄及電話方式通知受影響病人，九龍東醫院聯網亦已設立熱線5215 7326，供病人就事件查詢，熱線運作時間為星期一至日，早上九時至下午六時；病人亦可於非熱線運作時間留言查詢，職員會盡快回覆。

醫管局非常重視網絡保安，於發現事件後已嚴正檢視內部網絡系統，確認系統運作安全正常，事件不涉及網絡攻擊等因素。醫管局已即時暫停承辦商的系統維護工作。

醫管局持續採取多項措施強化醫療系統，包括持續提升網絡安全保障、用戶安全意識、重要關鍵基礎設施網絡安全、網絡監察及應變能力等，亦會與執法機構及網絡保安機構合作，提升網絡保安，以確保醫院運作、病人服務和個人資料安全獲得適當保障。醫管局亦呼籲受影響病人提高警覺，留意個人資料會被用作其他用途，作好個人資料保護，例如更改密碼等，有需要時可向警方求助。

完

2026年4月4日（星期六）  
香港時間14時58分

## 事件重點：

- 2026年4月醫管局確認病人資料外洩
- 涉及九龍東聯網超過56,000名病人
- 資料包含姓名、性別、身份證號碼、醫院檔案號碼及手術內容

## 官方回應：

- 已報警並通報私隱專員公署
- 暫停外判承辦商系統權限
- 初步表示不涉及外部網絡攻擊

## 風險啟示：

- 醫療資安包含內部與供應鏈風險
- 資料外洩可能流入暗網造成二次風險
- 需強化存取控制與監控機制

## 參考來源（可點擊）：

- [香港政府新聞網](#)
- [私隱專員公署](#)
- [明報新聞](#)

## How a Cyber Attack Becomes a Patient Safety Incident



Cyber Attack → Device Manipulation → Clinical Risk

Imagine a hacker  
breaking into your  
hospital.

Not to steal data. But to **control** a medical device inside a patient's body.

This is not science fiction. **It has already happened.**

心臟起搏器、胰島素泵、呼吸機——這些維持生命的裝置，如今已成為網絡攻擊的潛在目標。醫療資安不再是 IT 部門的議題，而是每一位醫療從業員都必須正視的患者安全課題。

PART 1 — 現實

# 醫院，已成為全球最大的 IoT 環境之一

現代醫院早已不再是單純的醫療場所。從連網醫療器材、遠端監測系統到雲端病歷平台，醫院已演變為一個高度互聯的網絡物理系統（Cyber-Physical System）。

## 連網器材

Connected Devices 遍佈全院，從 ICU 到門診

## 遠端監測

Remote Monitoring 讓臨床數據實時傳輸

## 雲端系統

Cloud Systems 儲存龐大的患者資料與影像

## 院內網絡

Hospital Networks 將所有設備串連成一體



# 連線能力 = 攻擊面

過去，醫療器材是獨立運作的機械裝置，物理隔離意味著安全。但今天，同樣的起搏器、輸液泵、呼吸機，已全面升級為連網裝置。

## 過去：獨立運作

- 心臟起搏器 (Pacemaker) — 無線通訊
- 輸液泵 (Infusion Pump) — 手動操作
- 呼吸機 (Ventilator) — 本機控制

物理隔離 = 天然防護

## 現在：全面連網

- WiFi 及 Bluetooth 遠端通訊
- 雲端數據同步與分析
- 遠端韌體更新 (Remote Firmware Update)

**Connectivity = Attack Surface**

## 2017 年：心臟起搏器漏洞事件

美國 FDA 發出安全警示，召回近 **46.5 萬枚心臟起搏器**。研究人員發現，這些裝置存在嚴重的網絡安全漏洞，令攻擊者可透過無線通訊介面入侵裝置。

### 未加密通訊

裝置與外部設備之間的通訊未經加密，攻擊者可輕易攔截及篡改數據

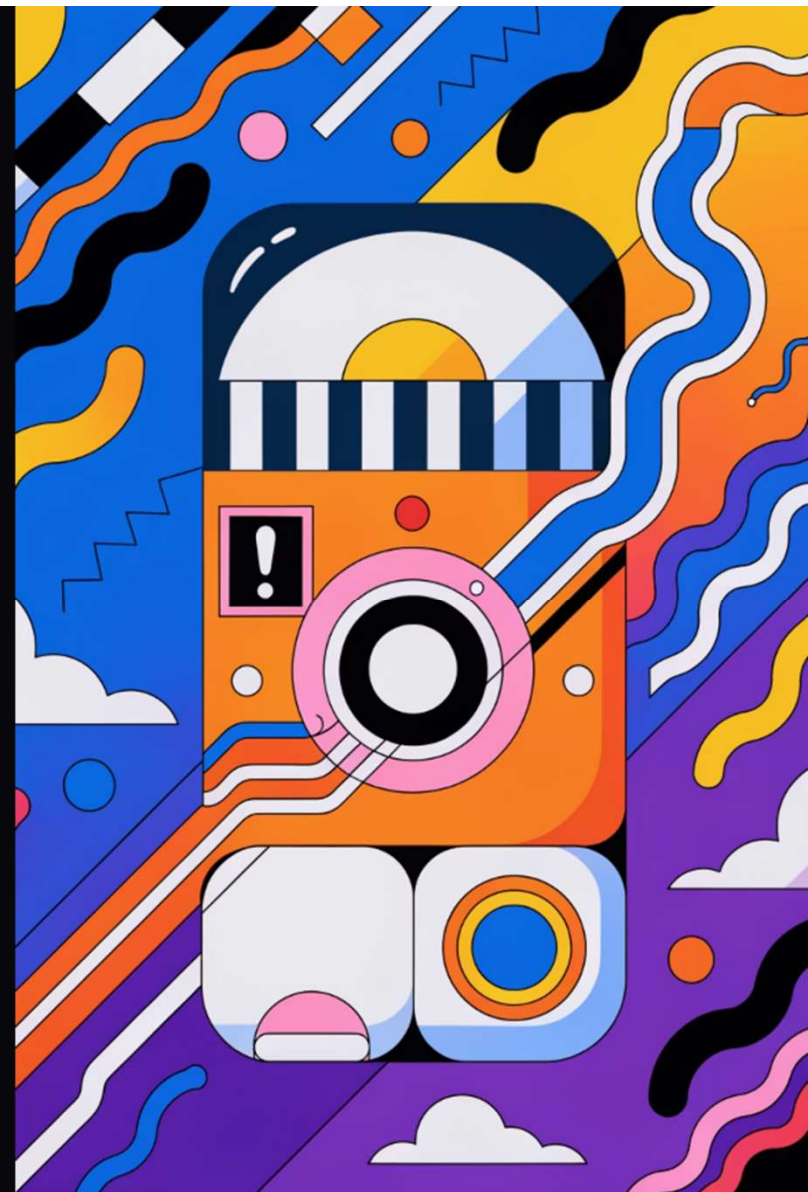
### 韌體更新可被攔截

遠端韌體更新機制缺乏驗證，惡意更新可被植入裝置

### 潛在後果

攻擊者可改變心跳設定，或發動電池耗盡攻擊（Battery Drain Attack），危及患者生命

- ❑ A medical device recall triggered by cybersecurity — 這是歷史上首次因網絡安全原因而大規模召回醫療器材。



PART 2 — 真實事故

## 2025 年：Contec / Epsimed 病人監護儀資安風險

### 風險重點

- FDA 2025 safety communication  
可被未授權遠端控制  
可能存在後門與資料外傳風險

FDA safety communication highlighted:

- **unauthorized remote control**
- **hidden backdoor behavior**
- **patient-data exfiltration risk**

One mitigation mentioned by FDA updates:  
remove network functions and keep local  
monitoring only.

### 為何重要

- 最貼近 bedside telemetry / patient monitor 場景  
說明醫療資安不只關乎隱私，更關乎資料完整性  
官方建議之一甚至是移除網路功能，只保留本地監測

---

官方 safety communication 已點名：monitor 資安問題可延伸到未授權控制與資料外傳。

## 醫院勒索軟件攻擊：當網絡癱瘓，手術要等待

全球多間大型醫院先後遭受勒索軟件（Ransomware）攻擊，後果遠超數據洩露——它直接中斷了醫療服務。



### 英國 NHS 大規模癱瘓

WannaCry 勒索軟件攻擊致使英國 NHS 系統全面癱瘓，超過 80 個醫療機構受影響，數以千計的預約及手術被迫取消。



### 美國醫院緊急停機

多間美國醫院因網絡攻擊被迫關閉電腦系統，影響醫學影像、患者資料及手術排程，部分患者被轉介至其他醫院。

**Cyber attack → Medical disruption.** 網絡事件的影響，已從數位世界蔓延至患者的床邊。

## DEMO — 模擬示範

# RPi3 + Arduino: Bedside Monitor Demo

先看真實事故，再看簡化 demo：重點是讓觀眾直觀看到資料完整性被破壞時，判讀如何被誤導。

## 示範目的

- bedside monitoring 場景
- telemetry replay / false vitals
- 連到 real-world integrity risk

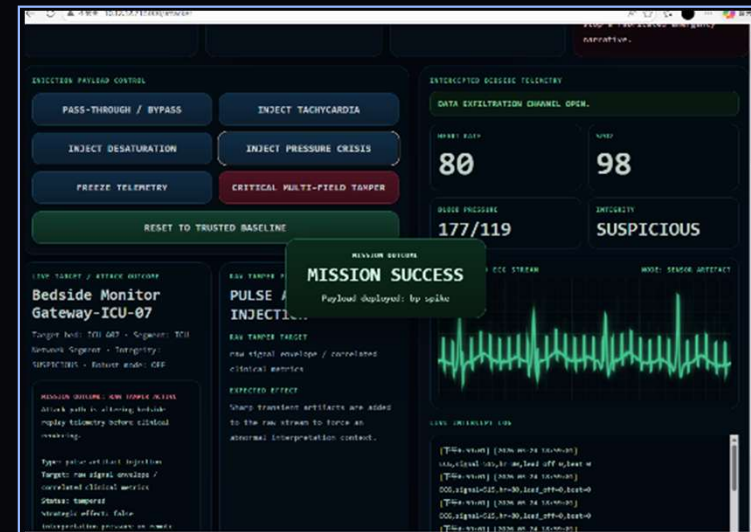
## 一句 takeaway

只要改變被相信的資料，  
就可能改變判讀與後續決策。

Wi-Fi: GL-MT300N-V2-121

Password: 90038978

Link: [Presidential ICU Device View Attacker Console](#)



Demo focus: telemetry freeze / false values / suspicious integrity flag

A simplified visualization of risk patterns that have already appeared in real medical cybersecurity incidents.

# 網絡安全 = 患者安全

這是本次分享最重要的一個觀點轉變。醫療器材的「安全」定義，必須與時並進。

## 過去的安全觀

Safety = 硬件故障防護

- 機械失效
- 電氣故障
- 環境因素

假設：意外 (Accidents) 是主要威脅

## 現在的安全觀

Safety = 網絡安全 + 軟件安全

- 網絡攻擊
- 惡意軟件入侵
- 遠端操控漏洞

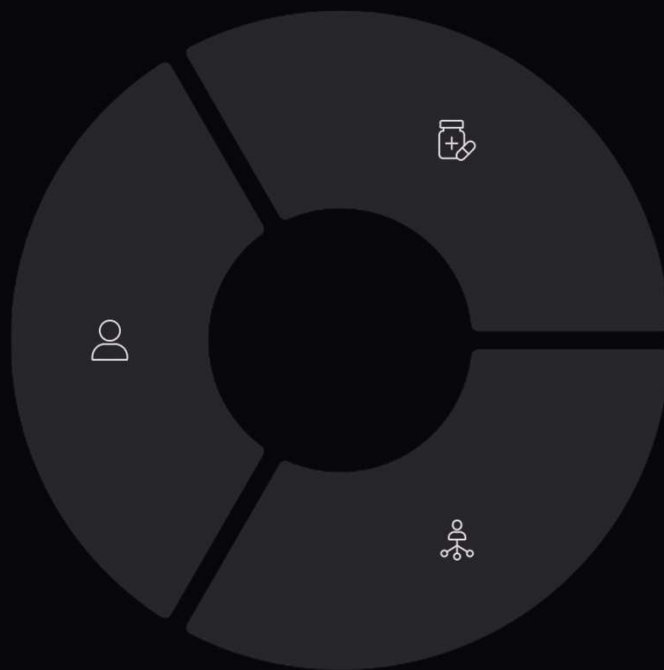
假設：攻擊者 (Attackers) 是真實威脅

Traditional safety assumes accidents. **Cybersecurity assumes attackers.**

## 醫療設備安全三角

現代醫療器材的安全，建立於三個相互依存的支柱之上。任何一個環節的失守，都可能令整個系統暴露於風險之中。

Patient  
患者安全是最終目標。所有安全措施的設計，必須以保護患者生命及健康為核心。



Device

醫療器材本身的軟硬件必須經過嚴格的安全設計與測試，確保裝置不被惡意操控。

Network

醫院網絡是連接器材與系統的橋樑，亦是攻擊者最常利用的入口，必須受到嚴密保護。

三者缺一不可——**Patient × Device × Network**，構成完整的醫療資安防護體系。

## 傳統醫療品質方法，為何不足以應對今日威脅？

傳統的醫療器材品質管理體系，是為應對物理世界的風險而設計的。面對蓄意攻擊的惡意行為者，這套框架存在根本性的盲點。

### ✓ 傳統質量所關注

- 電氣安全 (Electrical Safety)
- 電磁相容性 (EMC)
- 可靠性 (Reliability)
- 可用性 (Usability)

### ✗ 傳統質量所忽略

- 網絡安全威脅 (Cybersecurity Threats)
- 惡意行為者 (Malicious Actors)
- 蓄意攻擊的情境 (Adversarial Scenarios)

☐ Traditional safety assumes accidents. Cybersecurity assumes attackers.  
這句話，道出了兩套體系之間最根本的思維差異。



# IEC 81001-5-1：醫療健康軟件網絡安全生命周期標準

為填補傳統標準在網絡安全方面的空白，IEC 81001-5-1 應運而生。這是專門針對醫療健康軟件（Health Software）的網絡安全生命周期標準，為開發者提供系統性的安全開發框架。



## 核心理念

Secure Development Lifecycle（安全開發生命周期）——將安全設計貫穿整個產品開發流程



## 適用範圍

適用於所有醫療健康軟件及含軟件的醫療器材，涵蓋開發、維護至停用階段



## 監管地位

逐步成為各地監管機構（FDA、EU MDR）在評估醫療軟件資安合規性時的重要參考

## 標準的四大核心要素

IEC 81001-5-1 圍繞安全開發生命周期，定義了四個相互關聯的核心活動，確保醫療軟件在每個階段都得到充分的安全保護。



### 威脅建模

Threat Modeling：識別系統潛在威脅，評估攻擊向量與影響



### 安全需求

Security Requirements：定義可驗證的安全功能需求與非功能需求



### 安全設計

Secure Design：依照最小權限、防禦縱深等原則進行系統架構設計

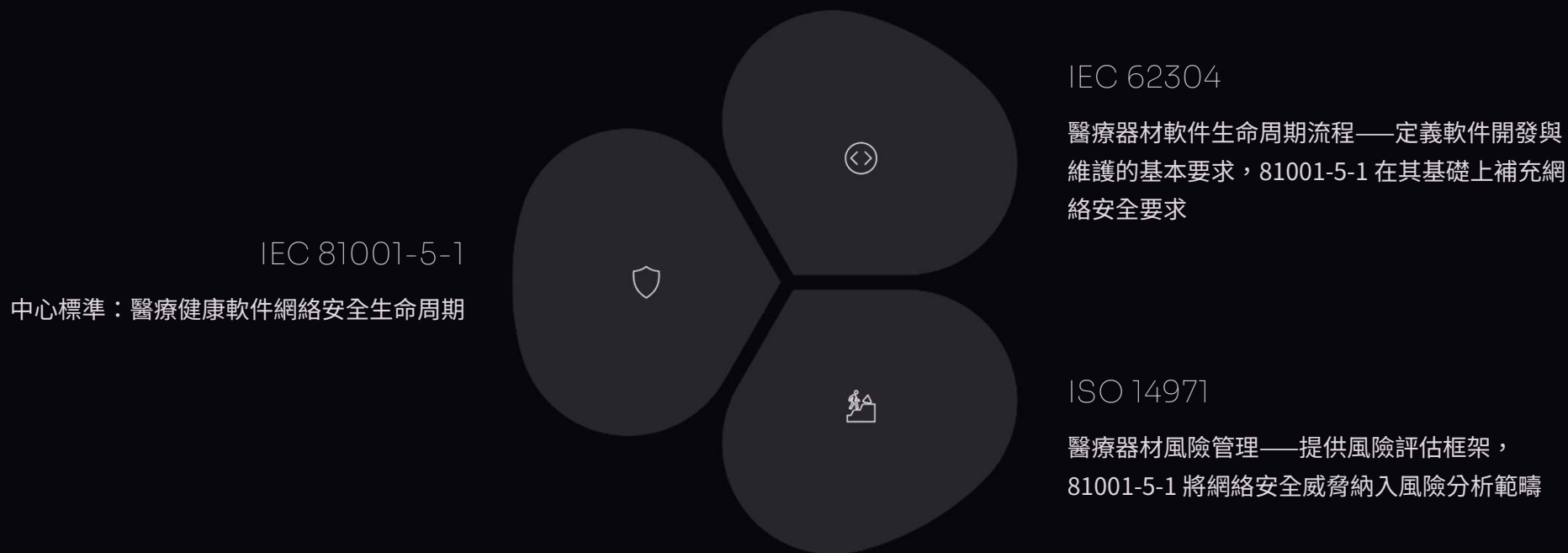


### 漏洞管理

Vulnerability Management：建立持續監測、披露與修補漏洞的機制

## 與相關標準的關係

IEC 81001-5-1 並非孤立的標準，而是與現有醫療器材法規框架緊密結合，填補了網絡安全這一關鍵空白。



三個標準協同運作，形成完整的醫療軟件**安全 + 品質 + 合規**管理體系。



#### PART 6 – 資安測試

## 醫療器材網絡安全測試：典型方法

符合 IEC 81001-5-1 及監管要求的醫療軟件，需要經過系統性的網絡安全測試。以下是四種核心測試方法，各有其獨特的目的與價值。

- ### 1 漏洞掃描

Vulnerability Scanning：自動化掃描已知軟件漏洞（CVE），識別系統中存在的已公開安全弱點
- ### 2 滲透測試

Penetration Testing：模擬真實攻擊者的手法，主動嘗試突破系統防禦，驗證安全控制措施的有效性
- ### 3 軟件成分分析

Software Composition Analysis（SCA）：識別第三方及開源組件中的已知漏洞，管理供應鏈安全風險
- ### 4 網絡安全測試

Network Security Testing：評估器材在醫院網絡環境中的通訊安全，包括流量分析與協議安全審查

## 測試目標：醫療器材的關鍵安全控制點

網絡安全測試並非泛泛而為，而是針對醫療器材最易受攻擊的核心控制點進行深入驗證。



### 身份驗證

Authentication：測試預設密碼、弱密碼政策、多因素驗證機制，防止未授權存取



### 加密機制

Encryption：驗證靜態數據及傳輸中數據的加密強度，確保敏感患者數據受到保護



### 韌體更新

Firmware Update：測試更新包的完整性驗證機制，防止惡意韌體被植入裝置



### 通訊安全

Communication Security：審查器材使用的通訊協議，識別中間人攻擊（MITM）等潛在風險

## 醫療器材的攻擊面全景

現代醫療器材的攻擊面，遠不止裝置本身。每一個與器材相連的介面，都是潛在的入侵點。全面的資安策略，必須覆蓋整個生態系統。

### 器材本體

Device 本身的操作系統、韌體、本地接口（USB、藍牙）及物理存取控制

### 雲端後台

Cloud Backend 儲存與處理患者數據，需防範未授權存取、數據洩露及服務中斷攻擊

### 配套手機應用

Mobile App 用於遠端控制或數據讀取，需防範 API 漏洞、本地數據儲存及通訊攔截

### 院內網絡

Hospital Network 作為所有器材的通訊橋樑，需防範橫向移動攻擊及網絡分段失效

PART 7 — 未來趨勢

## 監管趨勢：資安合規正在全球收緊

全球主要監管機構已將網絡安全明確納入醫療器材上市審批的必要條件。這不再是建議，而是強制要求。

### us FDA (美國)

- 2023 年《綜合撥款法》正式賦予 FDA 醫療器材網絡安全審查權力
- 要求提交 SBOM (軟件物料清單)
- 上市前必須提供安全測試報告及漏洞管理計劃

### EU MDR (歐盟)

- EU MDR 及 IVDR 要求醫療軟件符合網絡安全基本要求
- IEC 81001-5-1 被視為滿足合規要求的關鍵標準
- 網絡安全已成為 CE 標誌審批的評估範疇



## 網絡安全，已從選項變為義務

# Cybersecurity is now a regulatory requirement.

醫療器材製造商、軟件開發者及醫療機構，都必須重新審視自己的安全策略。過去，資安是「有更好，沒有也可以」的附加功能；今天，**沒有資安，就沒有上市資格**。

### 製造商必須行動

將 IEC 81001-5-1 納入開發流程，建立完整的安全開發生命周期

### 醫療機構必須準備

建立醫療器材資產清單與漏洞監測機制，制定事故應對計劃

### 監管者正在加速

FDA、EU MDR 等監管框架持續收緊，合規視窗正在縮小，及早行動比被動應對更為明智

結語 — CLOSING

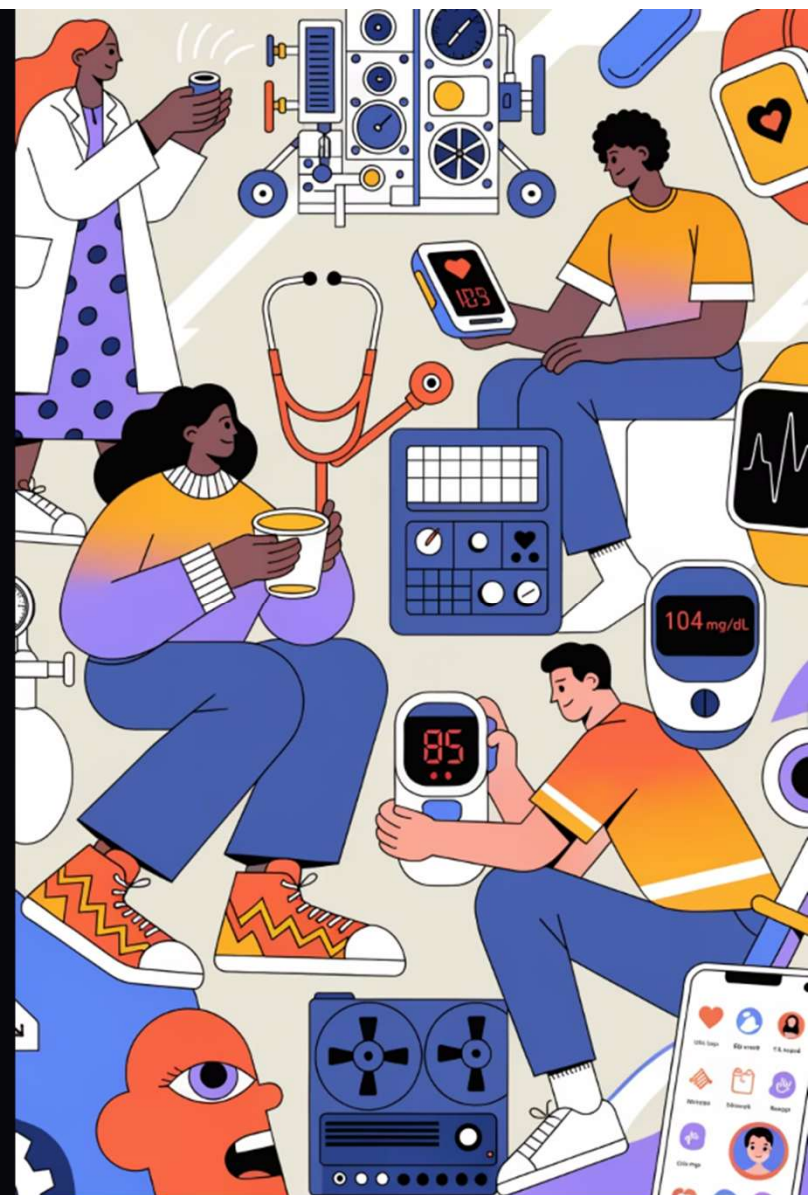
## 從機械裝置到連網電腦

Twenty years ago, medical devices were mechanical machines.

Today, **they are connected computers.**

這個轉變帶來了無可估量的醫療進步——遠端監測、精準治療、即時數據。但與此同時，它也帶來了我們從未面對過的全新風險。每一個連網的醫療裝置，都是一個需要被保護的入口。

我們這一代醫療從業員、器材開發者和資安負責人，肩負著一個獨特的歷史責任：在享受連網醫療帶來的紅利的同時，**守護每一位患者不因網絡漏洞而受到傷害。**



我們設計的，是信任

We are not only designing technology.

We are designing trust.

---

當我們設計醫療器材，當我們編寫醫療軟件，當我們建立醫療系統——我們不僅僅是在構建技術。我們在告訴每一位患者：**把你的生命交給這個裝置，是安全的。**

網絡安全，是我們兌現這份承諾的方式。

 CYBERSECURITY = PATIENT SAFETY