中醫藥從業員電子健康培訓課程 2009

深造班　第二節 – 個人資料（私隱）條例

講者：鄒錦沛博士

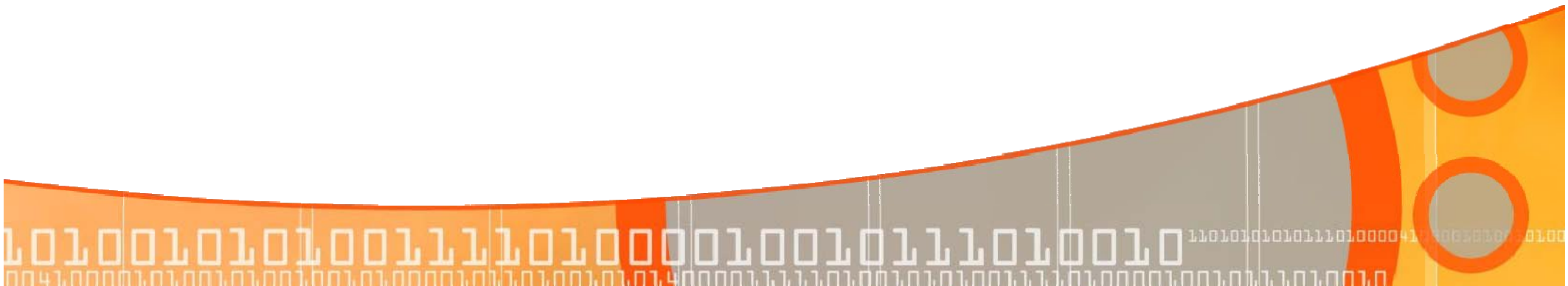
香港大學計算機科學系

資訊保安及密碼學研究中心

簡介

- 前言
- 個人資料（私隱）條例和數據保障原則
- IT安全和個人數據保障
- IT安全和保障資料原則之間的差距
- 中醫臨床時常見的資料洩漏及解決方案
- 總結

第一部：前言



警監會案例(2006年3月)

- 投訴香港警監會兩萬名市民個人資料在網上流傳

警監會承辦商涉違約判上判出事

伍健任董事 曾服務社署法援署

資料外洩事件

警監會電腦承辦商「判上判」導致資料外洩經過

球壇名人曾與足總對簿

警監會資訊署互推責任

2006年03月13日星期一

◆近五百名CSL客戶的資料在網上流傳。

82人查詢警監會洩密

《本報訊》投訴警方獨立監察委員會兩萬名市民個人資料外洩，個人資料在網上流傳，警方已透過國際刑警要求美國Google刪除網頁紀錄，但有網民卻將資料名單存檔，存放在個人網頁及在討論區上廣泛流傳，導致名單在網上杜之不絕。截至昨晚七時為止，已接獲八十二名懷疑個人資料被外洩的市民查詢。保安局局長李少光表示，暫無需要為受影響市民更換身份證。

投訴警方獨立監察委員會四人專責小組昨繼續

陳冠希不雅照泄露(2008年2月)

- 2008年2月，網民通過foxy共享陳冠希不雅照:你常會收到以下幾種信件嗎?
  - 當有新的相片出現在網上，他們用“趕往fox”和使用關鍵詞“新閃卡”傳遞消息
  - 用戶共享把這些不雅照放在一個命名為“新閃卡”的文件夾裏面

這些照片被一位自稱“奇拿”的人放在網絡上

醫院管理局

- 從2008年4月至2009年3月，很多案例涉及醫生丟失了USB「手指」，外泄了患者的個人資料

聯合外泄47病人資料

星島日報

(星島)2009年3月25日 星期三 06:30

(綜合報道)

(星島日報 報道)公共醫院去年發生多宗遺失病人個人資料個案，醫管局 雖已加強電腦系統保安及提供指引，但聯合醫院 前天再發生遺失載有病人資料的USB「手指」，一名醫生將四十七名病人的姓名、身分證號碼和年齡等，「抄錄」到自己的「手指」，作專業考試參考之用。聯合向受影響病人致歉，以及已向醫管局和個人私隱專員公署 呈報，初步調查相信該醫生沒有遵從資料保安守則，如發現任何人為錯誤，將作人事處分。

更多香港特區政府資料外洩的案例

- 2008-5：入境事務處部份“觀察名單” 在網站上洩露出來
- 2008-5：香港警方內部及機密文件被Foxy天王發現
- 2008-6：香港海關的機密文件被洩露出去

FOXY軟件泄政府機密 警內部手冊 高官出生日期一覽無遺

(明報) 04月 05日 星期六 05:05AM

【明報專訊】讀者爆料指出，警方及民航處的內部及機密文件被人透過網民廣泛使用的FOXY共享軟件上下載，其中包括連議員都無法索取的警察內部《程序手冊》、疑爲警長內部升級試的練習題及答案，甚至連民航處高官的出生日期等私隱資

共 1 張，顯示第 1 張

入境處機密文件外泄 網上任睇

(星島) 05月 08日 星期四 05:30AM

(綜合報道)

(星島日報報道)市民私隱外泄事件愈鬧愈大，入境處多份機密文件被發現上載至FOXY點對點分享平台，當中包括列入入境監視黑名單人士

Foxy天王再爆三大部門秘料

上週四，入境處十六份監聽黑名單的機密文件在搜尋器FOXY外洩，震動整個港府。翌日特首曾蔭權下令入境處要即時整頓，處長白韞六公開宣布已把所有機密資料剷走，確保不再外洩。

不過，同一名爆料人繼續在FOX...

究竟是什麼問題？

- 兩個主要來源：
  - 互聯網
  - USB手指碟

互聯網上的安全和隱私問題？

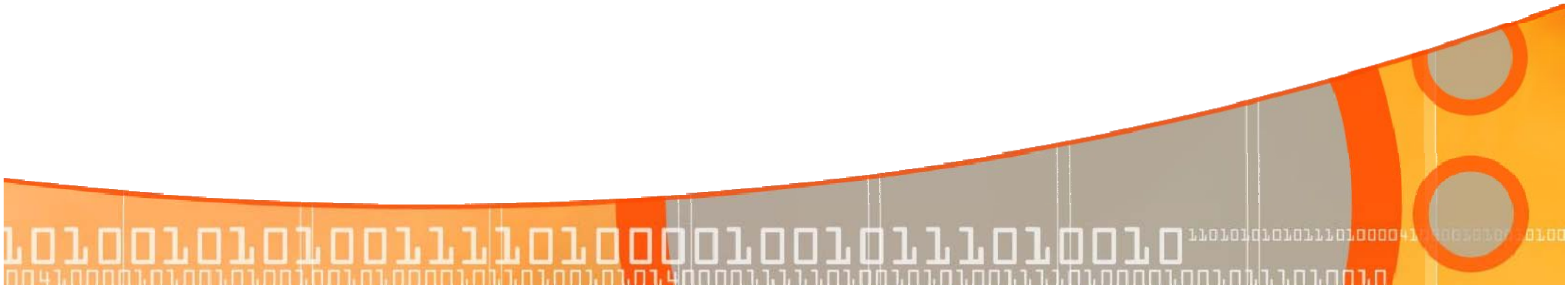
- 繼承了原始的互聯網 “ARPANET”：
  - 聯繫學術機構和研究機構的網絡
  - 沒有考慮安全和隱私的設計
- 從研究使用的網絡發展成為一個公共使用的網絡
  - 仍然以原來的基礎設施：TCP / IP 協定
  - “新”的服務支持：搜索引擎和檔案，新聞組，點對點
  - 惡意軟件：病毒，蠕蟲，間諜軟件，rootkit

互聯網用戶知道這些問題？

USB手指碟問題

- 太方便
- 沒有控制數據使用
- 使用者“不小心”

第二部：個人資料（私隱）條例和數據保障原則



個人資料(私隱)條例/私隱條例

- 1995年頒布，1996年12月20號生效
- 個人資料私隱專員負責監督
- 規定了個人、 公司、公共機構和政府部門對個人資料的搜集和使用。
- 該條例的關鍵要求是遵守6個保障資料原則
- 資料使用者不應違反保障資料原則使用或從事活動，除非該行為或做法是根據個人資料（私隱）條例規定或准許的。

六項保障資料原則

- 原則 1 – 收集個人資料的目的及方式
- 原則 2 – 個人資料的準確性及保留期間
- 原則 3 – 個人資料的使用
- 原則 4 – 個人資料的保安
- 原則 5 – 資訊須在一般情況下可提供
- 原則 6 – 查閱個人資料

關鍵術語

- **個人資料**：任何直接或間接與一名在世的個人有關的，從該等資料直接或間接地確定有關的個人身份及該等資料的存在形式令予以查閱及處理均是切實可行的
- **資料使用者**：控制該等資料的收集、持有、處理及使用的人
- **資料當事人**：指屬該等資料當事人的個人

原則1:收集個人資料的目的及方式

- 收集的目的
  - 個人資料是為了直接與將會使用該等資料的資料使用者的職能或活動有關的合法目的而收集
  - 資料的收集對該目的是必需的或直接與該目的有關的
  - 就該目的而言，資料屬足夠但不超乎適度，否則不得收集資料
  - 在資料收集期間，資料收集者必須採取一切切實可行的步驟，告知有關個人是否有責任提供個人資料，及未能提供的後果

原則1:收集個人資料的目的及方式

- 收集的方式
  - 在需要的情況下，收集個人資料的手段必須是合法和公正的:
    - 非法收集：未經授權截取郵件
    - 不公平的收集：未透露收集人身份的資料採集

原則2:個人資料的準確性及保留期間

- 所有個人資料必須**準確**，**最新**和**保存**的時間不得超過必要的時間
  - 準確：不正確，誤導，不完整，過時
- 每一個組織應該有一個**保存**策略，以及應該審核對電腦系統是否執行保留策略

原則3:個人資料的使用

- 個人資料只可用於在收集目的或直接有關的使用用途，除非資料當事人明確表示同意
  - 使用包括轉讓或披露

原則4:個人資料的保安

- 由資料使用者持有的個人資料應受到保護，防止未經授權的或意外的查閱、處理、 刪除或作其他用途
- 下列因素應考慮：
  - 該等資料的種類及如該等事情發生便能做成的損害
  - 儲存該等資料的地點
  - 儲存該等資料的設備所包含(不論是藉自動化方法或 其他方法)的 保安措施
  - 為確保能查閱該等資料的人的良好操守、審慎態度及辦事能力而採取的措施
  - 為確保在保安良好的情況下傳送該等資料而採取的措施

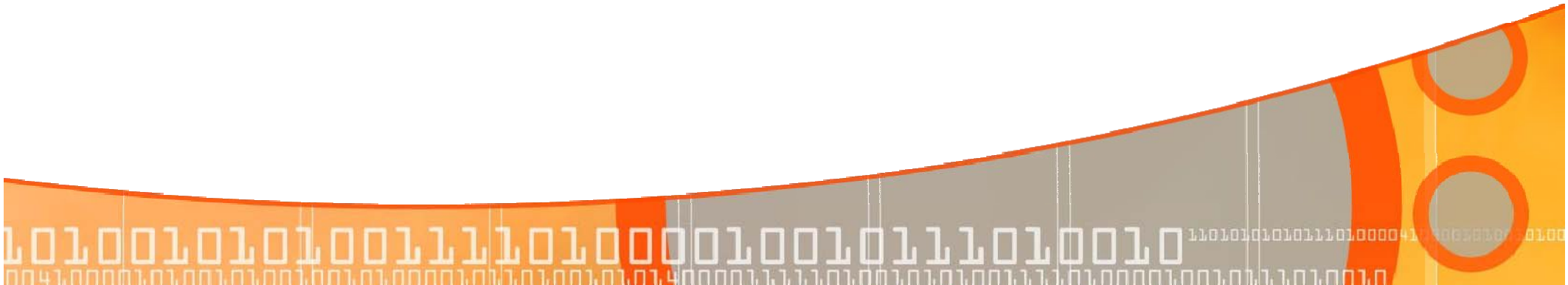
原則5:資訊須在一般情況下可提供

- 須採取所有切實可行的步驟，以確保任何人
  - 能確定資料使用者在個人資料方面的政策及實務
  - 能獲告知資料使用者所持有的個人資料的種類
  - 能獲告知資料使用者持有的個人資料是為或將會為甚麼主要目的而使用的

原則6:查閱個人資料

- 資料當事人有權
  - (a) 確定資料使用者是否持有他屬其資料當事人的個人資料；
  - (b) 要求
    - (i) 在合理時間內查閱
    - (ii) 在支付並非超乎適度的費用(如有的話)下查閱
    - (iii)以合理方式查閱
    - (iv) 查閱採用清楚易明的形式的、個人資料
  - (c) 在 (b) 段所提述的要求被拒絕時獲提供理由
  - (d) 反對 (c) 段所提述的拒絕
  - (e) 要求改正個人資料
  - (f) 在 (e) 段所提述的 要求被拒絕時獲提供理由
  - (g) 反對 (f) 段所提述的拒絕。

第三部：IT 安全和個人數據保障



IT 安全框架

- 使用控制（access control）
- 加密（encryption）

IT 安全框架 – 使用控制

- 可用性：防止未經授權隱瞞信息或資源
- 真實性：能夠核實數據的來源
- 問責制：審計信息必須是有選擇性保存和保護，因此可以追溯到影響安全的任何行動

IT 安全框架 – 加密

- 保密性：防止未經授權而披露的信息
- 完整性：防止未經授權的修改信息
- 不可否認性：當數據或消息在網絡上交換，發送者不可否認發送，接受者不可否認接受。

使用控制/加密是否解決問題呢？

- 使用控制
- 加密
  - 擁有硬件加密的昂貴的USB手指碟

二〇〇九年四月二十二日　星期三　夏曆己丑年三月二十七日

A2 要聞　蘋果日報 apple daily

花2250萬買加密手指 被指無助改變員工心態

防醫護洩私隱

■聯合醫院上月底及本月先後發生兩宗醫生遺失USB手指、洩漏病人資料事故。　資料圖片

【本報訊】為杜絕醫護人員遺失載有病人資料的USB手指等電子儲存媒體，醫院管理局建議斥資約2,250萬元，購買每支1,500元備有加密功能的貴價USB手指，預計供應1.5萬名員工使用。有醫管局董事局成員質疑，遺失病人資料是員工心態及文化問題，花錢買USB手指可能令員工以為很安全，繼續忽視守則、不尊重病人私隱。記者：陳沛冰 梁瑞琼

醫管局去年9月發生多宗遺失載有病服器存放病人資料，員工在醫院外可上網索取病人資料，不需使用USB手指，但該建議去年專責小組已提出。局方會簡化員工申領USB手指程序，可由行政總監以下的管理層批核申請。

文件指，醫管局會以「洗太平地」形式，要求所有員工刪除存於個人電腦及USB手指等不必要的病人個人資料。未來三個月先落實購買USB手指等措施，最遲7月中推行新懲處機制，即使用未經許可的電子儲存器或遺失，會被停職及停薪不多於兩周、書面警告及強制參加培訓課程；第二次違規會即時解僱。

令員工忽視守則

曾協助醫管局調查遺失USB手指的董事局成員莫乃光表示，之前該局已購入小量加密USB手指，可加密的很昂貴，

使用控制/加密是否解決問題呢？

- 醫生失去了她的USB手指碟，其中載有病人的個人資料加密

聯合產科女醫又失「手指」

(星島)2009年4月13日 星期一 06:30

(綜合報道)

(星島日報 報道)聯合醫院 不足一個月內，再有醫生遺失病人資料。醫院昨晚承認，上周六一名婦產科女醫生遺失了載有十一名孕婦資料及胎兒心跳掃描圖的USB「手指」，資料未有任何密碼或加密保護，院方已報警，初步相信是醫生沒有遵從資料保安守則。九龍東醫院聯網對事件深表遺憾和關注，及對受影響病人致歉。

針對員工遺失「手指」 私隱署為醫局辦培訓

(明報)2009年5月1日 星期五 05:05

【明報專訊】針對醫院屢次發生遺失載有病人資料的USB「手指」，個人資料私隱專員公署 下周起會為醫院管理局 的5.5萬名員工，舉辦歷年最大規模的行業私隱教育及訓練活動，教導前線人員如何處理載有病人資料的紀錄，以及認識有關法例。6月舉辦的亞太區私隱機構論壇亦會針對電子醫療記錄系統，將邀請食物及衛生局長周一嶽 參與討論。

教育活動為期一年

個人資料私隱專員吳斌說，去年1月起向15間醫療機構調查28宗遺失病人資料個案，涉及遺失載有病人資料的有USB閃存驅動器、手提電腦、數碼相機等。

他指出，去年已提出37項建議予醫管局 參考，但犯錯仍頻生，對此感到失望、無奈，故會為醫管局舉辦為期一年的教育活動，由醫管局總部開始，再到其轄下醫院及診所，為前線人員舉辦培訓講座。

第四部：IT 安全和保障資料原則之間的差距

香港個人資料（私隱）條例

保障資料原則	
	IT 安全框架
原則 1 – 收集個人資料的目的及方式	×
原則 2 – 個人資料的準確性及保留期間	×
原則 3 – 個人資料的使用	×
原則 4 – 個人資料的保安	√
原則 5 – 資訊須在一般情況下可提供	×
原則 6 – 查閱個人資料	×

他們解決了哪些問題?

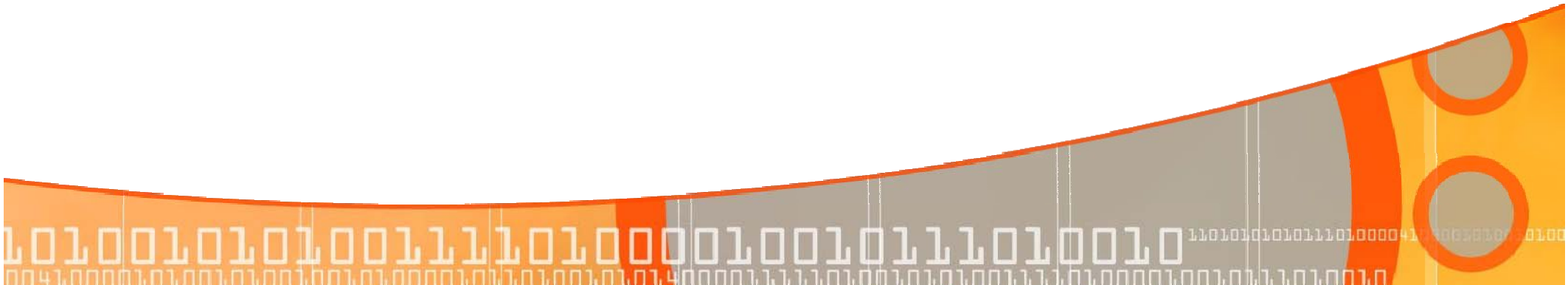
- IT安全框架唯一解決了“個人資料的保安”的安全問題
- 它僅僅解決了“他們的”問題，而沒有解決“合適的”問題
  - 典型的軟件工程問題

技術和數據保障原則

- 應該由不同的技術來實現:

原則	技術
原則 1 – 收集個人資料的目的及方式	要求新的技術和框架（目的性的和有約束力的）
原則 2 – 個人資料的準確性及保留期間	
原則 3 – 個人資料的使用	
原則 4 – 個人資料的保安	IT 安全 （安全性和問責制）
原則 5 – 資訊須在一般情況下可提供	用戶接口技術 （用戶權利和數據的準確性）
原則 6 – 查閱個人資料	

第五部：中醫臨床時常見的資料洩漏及解決方案



使用人手記錄的診所

- 診所
  - **常見問題：** 因病人記錄放在容易被接觸的地方
  - **解決方案：**
    - 存放在上鎖的柜
    - 記錄存放地方只能給有權人士進入
    - 診治及配藥後立即存放
    - 在第二位病人進入診治前把前一位病人記錄收藏
  - **常見問題：** 遺失
  - **解決方案：**
    - 存取需要在記錄簿上記錄並簽署
    - 只容許有權人士存取記錄

使用人手記錄的診所

- 口頭
  - **常見問題:** 經醫師或護士口頭洩露
  - **解決方案:** 醫師及護士需嚴守專業守則，在沒有病人的許可下不得向第三者（包括病人家人在內）透露病人的有關資料

- 運送
  - **常見問題:** 遺失
  - **解決方案:**
    - 給有商譽的傳送者
    - 發件及收件需簽署
  - **常見問題:** 給無權人士查看
  - **解決方案:** 有適合的包裝、在包裝外蓋上印章

使用電子記錄的診所

- 電腦
  - **常見問題:** 給無權人士查看
  - **解決方案:**
    - 螢光幕只面向醫師
    - 安裝有密碼的螢幕保護
    - 需要密碼進入診病系統
- 資料庫
  - **常見問題:** 遺失或給無權人士查看
  - **解決方案:**
    - 存取資料日誌
    - 資料庫需有密碼保護
    - 伺服器需存放在上鎖的房間內

使用電子記錄的診所

- 經互聯網
  - **常見問題：** 遺失或給無權人士查看
  - **解決方案：**
    - 安裝防火牆
    - 安裝防病毒軟件
    - 安裝防駭客入侵監察系統
    - 把資料庫加密

第六部：總結

使用數據庫中個人資料的建議程序

- 所有使用數據庫中的個人資料應有授權，監督和交代
- 所有複製/備份有個人資料的數據庫，應有授權，監督和交代
- 所有從包含個人資料的數據庫導出數據，應有授權，監督和交代
- 所有上述報告的數據庫操作，應製作並定期檢討

導出數據的建議程序

- 導出個人資料，應授權
- 導出個人資料到可移動存儲媒體，例如磁盤，光盤，USB手指碟，應該有適當的標籤
- 電腦打印的副本，其中包含個人資料，應該包含適當的標籤
- 電子郵件，其中包含個人資料，應該有內容加密和適當的標籤

銷毀個人資料的建議程序

- 保留個人資料在IT系統的期限應按照有關法律及監管要求和行業標準
- 每當個人資料不再使用，應妥善銷毀
- 對於包含個人資料的電腦 /服務器，PC /服務器的硬碟應徹底銷毀
- 所有的備份和導出的副本，應予以銷毀
- 所有打印的副本應銷毀
- 對於銷毀的記錄應該妥善保存

多謝

課後討論時間