

# The Risk Management of Medical Information

醫療資訊的風險管理  
江坤祥

1

## 內容綱要

- 醫療資訊常見的系統風險
- 資訊系統風險評估
- 本院醫療資訊風險管理措施與作為

2

## 資訊的形式

- 書寫或列印於紙上。
- 儲存於電子媒體上。
- 以郵寄或電子媒體傳輸。
- 顯示於影片或圖片中。
- 在對話當中。

無論資訊的形式是什麼，都應該受到適當的保護。

3

## 資訊風險的風從哪裡來？

- 因為你的資訊有\$\$\$\$\$。
- 因為你的資訊影響到對方。
- 因為你的資訊會產生特定目的。
- 因為你的設備好玩。
- 因為你的系統不設防。
- 因為你不小心。
- .....

4

## 醫療資訊常見的系統風險

- 系統密碼交予他人。
- 病人資料無意間外洩。
- 輔助提示資訊不足。
- 流程變動，系統漏洞。
- 人工作業流程的生疏。
- 駭客與電腦病毒攻擊。
- 系統故障與資料毀損。
- 未落實資訊品管。
- 系統文件不夠完備。
- 違反電腦軟體使用規定。
- 委外服務的專案管理。
- 資訊分享的界限。
- 政府的法令規章。
- 資訊系統的導入時機。
- 設備安全。
- 資訊人員管理。

5

## 密碼外洩

6

## 密碼外洩

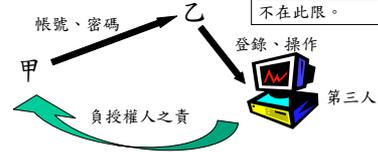
- 貪求方便。
- 記性不好。
- 輕忽資訊的無形價值。
- 密碼編碼過於容易。
- 簡易編碼法：5j/cj86aup6eji3

7

## 密碼外洩所帶來的威脅

- 系統安全出現漏洞。
- 資料有遭到竄改之虞。
- 表見代理

民法第169條  
由自己之行為表示以代理權授與他人，或知他人表示為其代理人而不為反對之表示者，對於第三人應負授權人之責任。但第三人明知其無代理權或可得而知者，不在此限。



8

## 病人資料外洩

9

## 資料外洩的代價

【台北報導】針對日來爆出逾二千萬筆民眾個人資料外洩，中華電信、遠傳等七家電信業者昨坦承有疏失，將主動通知資料遭外洩的民眾，以及提供免費更換電話號碼等補救措施。中華電信並允諾將減免月租費、通話費，還額外補償消費者一筆金額。

消保會法制組長黃宏全指出，根據《消費者保護法》第七條，業者本應當對消費者造成的損害負起無過失賠償責任，不論是由不肖員工將資料外流或是委外業務公司外洩。根據《民法》規定，電信公司都要負責到底，消費者可要求懲罰性賠償。另也可依《電腦處理個人資料保護法》，消費者可求償二萬到十萬元損害賠償。

10

## 預估損失

業者提出之補償方案

減免三個月月租費→  $88 \times 3 = 264$

損失金額→  $10,000,000 \times 264 = 2,640,000,000$

法律規定之賠償方案

個人資料保護法→  $20,000 \times 10,000,000 = \text{??????}$

民法懲罰性賠償→ 依個案 ??????

11

## 個人資料的市場行情

資料內容	價格(元/筆)
電子郵件位址	0.2~0.5
姓名、身分證號碼…(一般)	1~3
姓名、身分證、生日、地址、電話…(完整)	3~10
名人隱私…如罹患某種不名譽之病	500~3000

12

## 個案分享

- 提款存根
  - 帳號、餘額→個人經濟狀況
- 便條紙
  - 病歷號、年齡、主診斷→健康狀況
- 電腦報表
  - 具有特定目的資訊
- 磁片、光碟片、網路
  - 大量且詳細的個人基本資料

13

## 駭客與電腦病毒攻擊

14

## 駭客入侵

- 探察：尋找目標。
- 掃描：尋找漏洞。
- 漏洞利用：利用目標的系統弱點。
- 主機存取：對目標進行資料複製、竊取、竄改、破壞等動作。(如：Spyware…)
- 安置後門：暗藏伏兵。(如：Trojan…)
- 阻絕服務：頻寬消耗、資源耗竭、系統癱瘓。

15

## 電腦病毒

- 為了惡意破壞或竊取資料而設計的小程式。
- 種類：
  - 電腦病毒(Computer virus)
  - 電腦蠕蟲(Computer worm)
  - 特洛伊木馬(Trojan horse)
- 目前大都以混和型態出現
  - Virus + Worm
  - Trojan + Worm

16

## 電腦病毒攻擊大事紀

時間	病毒名稱	特徵	全球損壞電腦	全球損失預估	國內受害者代表
2001.10	Nimda	LAN	800萬部	6億美元	
2002.4	Klez	E-mail	∞	∞	
2003.8	Blaster	LAN	140萬部	30億美元	
2004.2	Beagle_X	E-mail	∞	∞	
2004.2	Netsky_AB	E-mail	∞	∞	
2004.5	Sasser	LAN	1800萬部	∞	

17

## 電腦病毒攻擊

- 途徑：磁片→網路
- 誤開或預覽來歷不明的檔案
- 未使用或未更新防毒軟體
- 影響：
  - 檔案遺失、效能降低。
  - 院內群聚感染。
  - 網路流量大增。
  - 系統不穩或停止服務。

18

## 高科技犯罪

- 面對駭客攻擊與防禦，「視同作戰」。
- 最想獲得何種資料？(What)
  - 個人基本資料
    - 帳號、密碼
  - 通訊錄
  - My Documents
  - 整顆硬碟的資料

19

## 高科技犯罪

- 哪些人最容易得手？(Who)
  1. 資訊人員
  2. 委外廠商
  3. 電腦操作員
  4. 高階主管
  5. 資深電腦駭客

20

## 高科技犯罪

- 為何容易得手？(Why)
  - 科技日新月異，防不勝防。
  - 未明確劃分存取權限。
  - 系統設計時的方便或疏忽。
  - 未建立相關稽核機制。

21

## 資訊系統風險評估

22

## 資訊系統風險評估

- 沒有絕對安全的系統，只要系統具有價值性就意味著風險即將來臨。
- 通過HIPAA或ISO 17799就能保證系統安全無虞？
- 雖不能達到「絕對安全」，但可做到「相對安全」。
  - 能阻止絕大多數的資訊安全事故。
  - 將事故對組織的負面影響降至最低。
- 保護對象：
  - 系統、資料、存取通道、運算資源。

23

## 資訊系統風險評估

- 風險等級評估
  - 資產的價值
  - 威脅的可能性
  - 弱點的大小
  - 發生的機率
  - 對組織的衝擊

24

## 資訊系統風險評估

- 本院資訊系統風險等級：

25

希望全員重視數位資產，共同營造一個安全的  
資訊安全措施，今天不做，明天還是要做...

26

# 財團法人仁愛綜合醫院 風險管理課程 資訊安全基本能力測驗

單位：

卡號：

姓名：

得分：

## 是非題

- 1.( )有關資訊安全的威脅，凡將個人資訊不正當收集或擅自公開稱之為侵犯隱私權。
- 2.( )為確保資訊安全，系統使用者的管理對策，並不包含設定使用者密碼。
- 3.( )對於網路系統的使用，限制員工對外連絡權限為正確的觀念。
- 4.( )Internet 是一個完全隱密的開放空間，不論是瀏覽網站、下載軟體元件、收發電子郵件以及網路購物，都不需要安全的顧慮。
- 5.( )在系統安全防護作業中，包含引進防毒軟體。
- 6.( )下列項目中，ABDFG 是威脅資訊系統安全的因素。A.天災 B.軟硬體系統故障 C.電磁信號外洩 D.通信線路竊聽 E.儲存媒體外洩或破壞 F.資訊中心場地安全 G.人為入侵破壞。
- 7.( )添購不斷電(UPS)系統不屬資訊系統安全災害防治措施。
- 8.( )要防止人為進入系統惡意破壞或偷取資料，可採取 ABCD 四項措施。A.設定密碼 B.資料加密 C.對每個用戶設定使用權 D.對檔案設定保護模態 E.裝設不斷電系統(UPS)
- 9.( )為保障資訊安全，在公司管理制度中應雇用值得信賴的人員。
- 10.( )為了防犯電腦從業人員產生電腦犯罪的動機，資料存取應依職務設定權限等級。
- 11.( )人工檢查資料輸入是否正確，是屬於資料安全管理。
- 12.( )電腦系統在遭遇當機或損害一時無法修復，而系統又不能停機太久時，可採用人工作業方式緊急處理。
- 13.( )通常在資料輸入時，每間隔一段時間就需安排一個檢查點，以便資料遭到破壞時可隨時將備份資料還原繼續作業。
- 14.( )完善的資訊安全系統，應在使用者資料、作業系統和電腦來源，設立足夠的關卡，以防止使用者透過程式去使用不是他自己的資料，此即獨立性的概念的(Isolation)。

## 選擇題

- 15.( )在資訊安全的種類中，有關媒體出入管制項目，是屬於下列何者的重要項目之一？(1)實體安全(2)網路安全(3)法律安全(4)系統安全。
- 16.( )為了防止因資料安全疏失所帶來的災害，一般可將資訊安全概分為下列四類：(1)實體安全，網路安全，病毒安全，系統安全(2)實體安全，網路安全，資料安全，系統安全(3)實體安全，資料安全，人員安全，電話安全(4)實體安全，資料安全，程式安全，系統安全。
- 17.( )何者是錯誤的「電腦設備」管理辦法？(1)所有設備專人管理(2)定期保養設備(3)允許使用者因個人方便隨意搬移設備(4)使用電源穩壓器。
- 18.( )電腦犯罪的敘述何者為誤？(1)犯罪容易察覺(2)採用手法較隱藏(3)高技術性的犯罪活動 (4)與一般傳統犯罪活動不同。
- 19.( )下列何者不是資訊系統安全之措施？(1)備份(2)稽核(3)測試(4)識別。
- 20.( )下列何者屬於惡意破壞？(1)人為怠慢(2)擅改資料內容(3)系統軟體有誤(4)系統操作錯誤。
- 21.( )災害復原階段，首要的工作為(1)軟體的重置(2)環境的重置(3)系統的重置(4)資料的重置。
- 22.( )下列那一項動作進行時，重新開機會造成檔案被破壞的可能？(1)程式正在計算(2)程式等待使用者輸入資料(3)程式從磁碟讀取資料(4)程式正在對磁碟寫資料。
- 23.( )資訊之人員安全管理措施，下列何者不適宜？(1)銷毀無用報表(2)訓練操作人員(3)每人均可操作每一電腦(4)利用識別卡管制人員進出。
- 24.( )下列有關防火牆之敘述何者為誤？(1)防火牆無法防止內賊對內的侵害，根據經驗，許多入侵或犯罪行為都是自己人或熟知內部網路佈局的人做的(2)防火牆基本上只管制封包的流向，它無法偵測出外界假造的封包，任何人皆可製造假的來源住址的封包(3)防火牆無法確保連線的可信度，一但連線涉及外界公眾網路，極有可能被竊聽或劫奪，除非連線另行加密保護(4)防火牆可以防止病毒的入侵。
- 25.( )災變復原計劃，包括下列何者之參與？(1)程式設計人員(2)組織全員(3)系統操作人員(4)資料處理人員。