【政風宣導-公務機密宣導】電子病歷的安全防護

廉政檢舉專線：0800-286-586

美國研究機構 Ponemon Institute LLC 對 80 家美國醫療機構進行訪查後，於 2012 年 12 月發布了一份對病人隱私及個人資料之安全防護所做的研究報告。報告中顯示：有高達 94%的醫療機構在過去兩年內曾經發生病患資料遺失或遭竊取的事故，有將近一半（45%）的受訪醫療機構在兩年內發生 5 次以上資料遺失或遭竊取的事故。而最常遭竊或遺失的資料，是病患的保險紀錄和病歷。

常見的事故發生原因包含硬體設備遺失、員工或第三方使用者操作失當、員工監守自盜，以及駭客入侵等。超過 50%的受訪機構表示自身並沒有偵測或監控資料是否遺失或外洩的能量，致使全美醫療體系在一年中，因資安事件所遭受的財務損失即達 70 億美元。

美國雖然是科技大國，各項科技均領先群雄，且資訊科技的發展亦為世界翹楚，然而，從研究資料中卻發現：美國醫療機構的資訊安全防護竟是如此不堪一擊。國內目前雖未見到相關研究，但是，他山之石可以攻錯，見到別人的缺失，我們可以引以為鑑。

資訊安全的標的可分為有形與無形兩種，以前述案例而言，有形的標的包括資訊設備、紙本的病歷等看得到的東西；無形的標的則如電子病歷等儲存在電磁媒體中的資料。由於網路的發達，資訊共享已是一種常態，因此，電子病歷已是一種無法可擋的趨勢。既然是時代的潮流，不能走回頭路，所以就必須針對它的安全性做全面的規劃。

對於網路伺服器的安全，雖可透過防火牆加以保護，惟駭客的手法日益增強，正所謂道高一尺、魔高一丈；而電子病歷又是個人資料保護法所保護的標的，因此對於個人資料的保護，不能全部仰賴防火牆。

我們既然無法完全防止駭客入侵資料庫竊取機密文件，就要想辦法讓駭客入侵後，所竊取的文件無法看懂，因此，對於電子病歷的資料，可以採用加密方式處理。

首先針對醫生、護士、藥劑師及行政人員，給予不同權限的憑證，依權限授予不同的功能，例如醫生可以讀、寫病歷，藥劑師就只能看到處方；醫生在看診後，把病人的病情記錄在電子病歷上，在存檔時，即以他的憑證把檔案加密，同時留下簽章紀錄。經過加密後的檔案，即使被駭客入侵竊取，或是員工監守自盜，縱使拿到檔案，但因沒有解密金鑰，打開檔案後，看到的都是亂碼，所以就算防火牆擋不住駭客，資料被偷走，拿到的資料也是有字天書，讓人看不懂，即可達到保密的目的。而透過電子簽章的方式，讓每個修改過病歷的人，都用他自己的憑證，經由特定的加密演算法，記錄修改的時間及人員，如此一來就可避免人為竄改資料的情事發生。

其次，也要防止具有權限的人員，濫用權限竊取資訊。例如有讀取權限的工作人員，利用其合法權限，把電子病歷列印後流出。所以在設定權限時，可以限制列印的功能，讓一般人員無法列印病歷，以防止合法人員的危安事件。為避免因電腦遺失造成電子病歷資料外洩的風險，在規劃電子病歷系統時，即應考量設置檔案伺服器(File Server)，將電子病歷集中存放在機房的資料庫中；而機房除了專人管理外，也要有門禁管制措施，記錄每日之進出人員及進出時間，並避免閒雜人等隨意進出，造成危安事件。

除此之外，電子化的病歷，最怕的是資料損壞、遺失，因此，對於電子病歷還是要每天做備份（Backup），以避免因為資料庫毀損而造成資料遺失，損及病人權益。又備份不能只做一份，醫院也應有異地備援（Remote Backup）的觀念，要在不同的地方也儲存備份，以防自己的機房遭到意外時，還有另一份資料可以用。

電子化企業已是一個趨勢，醫院也無法置身其外；面對資訊科技的進步，電子病歷已是無可避免，唯有事先妥慎規劃及萬全準備，才能確保病患的個人資料不外洩。

-轉載自清流月刊

109.12

新北市八里區公所政風室關心您