議題觀點

字級調整 小 中 大

2007/1/23

從HIPAA經驗看台灣醫療資訊安全管理

陳怡如、梁芷瑄 ( )

網際網路的盛行已有十多年的歷史，各行各業無不跟上這股風潮，利用網路這項工具來達到降低成本、提高效率的目的。就連一向被認為對接受新科技較保守的醫療業，也早就使用電腦以及網路技術來增加工作的效率，以期藉著減少人力及紙上作業的方式，降低些許成本。像是網路掛號、保險人資格的確認、線上病歷、付款、醫療用品的採購等，都從以往的人工作業，慢慢的轉向在網際網路上提供服務。

為了規範其中的資訊安全，美國國會於1996年通過了健康保險可攜性與責任法案 (Health Insurance Portability and Accountability Act, HIPAA)，它規範了資訊安全性與機密性，還有符合保護個人隱私的需求，並明訂相關業者之資訊系統應該有的安全機制。HIPAA的內容分為四個部分（黃妙慧、張克章，民95）：

1. 管理程序：管理程序指的是為了保護資料所做的安全考量，並依據此程序指定專責的人員來執行資料保護的工作，並記載於正式的文件上面。管理程序有以下十二項規範：認證、聯盟間安全協議、應變計畫、處理紀錄的正式機制、使用者權限、內部稽核、人員安全、安全組態管理、安全事件處理程序、安全管理程序、結束程序以及訓練。

2. 實體防護：實體防護有四種規範，分別為指定安全責任、媒體控管、實體使用控制、工作站管理政策。其目的在於維護資料的完整性、機密性和有效性。

3. 技術安全服務：此目的也在於維護資料的完整性、機密性和可用性，還包括保護、控制及監督使用資訊的程序。一共有五項規範，使用權限控制、稽核控制、授權控制、資料確認以及實體確認。

4. 技術安全機制：內容有網路控管一項。其目的在防範透過網路未經授權使用資料作業的程序。

HIPAA的規範，除了醫療診所要遵守之外，任何的醫療保健機構、資訊交換中心，或是以電子方式處理醫療相關資料的使用者都必須遵守。另外，與這些機構有業務往來，而且在業務過程當中也使用到受保護的醫療資訊 (Protected Health Information, PHI) 的機構，也在HIPAA的規範之內。

除了管理方面的規範之外，軟硬體的支援技術也是不可或缺的。包含了電子化醫療交易與編碼標準 (Transactions and Code Set, TCS)、隱私權規範、安全規範以及唯一識別碼。其中TCS規定醫療業者必須使用預先訂定的通訊與交易的電子化交換標準，也規定要使用一組標準的編碼，進行醫療交易相關的診斷和服務。隱私權的規範是在所有特定情況之下，可以使用或公開個人醫療資訊(PHI)，保護病患對自己醫療資訊保密的權利，並讓他們可以控制PHI的使用方式及公開的條件。安全規範提供在電子化環境中，保護PHI的技術需求與運作程序，也就是如何保持其安全，維持其完整性，並且能在需要的時候被取得。唯一識別碼是用來識別員工、醫療計畫、業者以及病患。各個醫療機構會有獨特的識別碼，而且將會使用集中化的系統進行分配與管理。

HIPAA擁護者認為，HIPAA的規範兼顧軟硬體及管理規範，看起來十分周全，對於IT產業以及顧問公司來講，又是一筆很大的商機，其目前預估的產值從10億170億美元不等，可以大幅提升經濟的發展；而且虛胖和官僚的醫療機構，將會因為新系統在效率上的改善，而馬上讓投資回收。IBM的醫療產品總經理Russell Ricci就曾表示，政府所頒布的這些法令，將讓高科技產業實際改善醫療產業的品質、安全以及成本效益。即便有許多人為HIPPA的通過感到十分樂觀，但HIPAA截至目前為止所引發的爭議仍是相當的大 (Junnarkar, 2003) 。

根據美國健康資訊管理協會 (American Health Information Management Association, AHIMA) 的調查指出，完全符合HIPAA規範的醫療相關機構大約維持在40%左右，但其結果也指出，未達規範標準 (HIPPA compliance <85%) 的機構，從2005年的9%升高到2006年的15%。這是一個警訊，顯示醫療產業的配合程度無法完全與政府政策相呼應。受訪者認為，最大的一個障礙來自於資源的缺乏，尤其是訓練以及教育新的員工方面。在AHIMA的調查結論中提到，即使許多處理隱私權問題的執掌單位已經盡他們最大的努力，但這些醫療相關機構本身並不把隱私權列為優先考量的重點，所以當他們要求支援或是資源的時候，該機構卻總是不加以理睬，以至於他們的需求或建議無法實行 (AHIMA, 2006)。

另外，紐約州奧爾巴尼郡 (Albany) 聖彼得醫療服務中心的網管人員Zimmerman也提到：「如果要真的達到法律規定的安全與隱私規定，光是人事與相關技術的成本就是一筆天文數字。而且法令內容過於鬆散，因此要怎麼做才算符合法令也令人頭痛」。再來是關係到醫療產業的特性，由於對醫療產業該付出的整體成本過於樂觀，但取得法律支持的同時卻沒有相關的補助措施，使得政府機構飽受抨擊。電子資訊安全公司 (Mirapoint) 的全球應用工程主任Tim Chiu也提到，HIPAA的內容相當混亂，到底有哪些是要達成的規定、期限是何時、要花費多少預算等等，都有不同的說法 (Junnarkar, 2003)。

ThruPoint的安全顧問Ben Rothke將HIPAA與美國2002年通過的沙賓法案(The Sarbanes-Oxley Act)[1]拿來做比較，他認為HIPAA比起沙賓法案，不但缺乏獎勵與罰則，無法完全保障病人的就醫紀錄，也由於處罰的對象不及高層，讓執行長沒有遵守法案的迫切利害關係。他說，「HIPAA之所以那麼沒用，責任要歸咎於國會，因為它不僅逃避了強制責任，還開了一個後門讓執法人員可以存取該法案理當保護的病人資料。」故他覺得大多數人都會同意，個人醫療照顧的資訊仍處於高度風險之下 (Rothke, 2005) 。

雖然關於HIPAA的爭議不斷，但其保障醫療資訊安全的美意實在值得國內相關單位跟進。其實國內之前早已針對HIPAA的條文來進行研究，評估是否要依據HIPAA的法案條文來制訂相關的規範。然而，由於美國與台灣的民情不同，制度也有所差異，比方說，美國是屬於私人保險制度，保險公司與多家醫療機構存在契約關係，造成被保險人與醫療院所產生許多轉換的問題，而國內採用的是健保制度，屬於單一保險人方式，所以不需要考慮轉換的問題。在幾經考量之下，國內目前擬訂的是「醫療資訊安全與隱私保護指導綱領草案」，有九大原則，十二條條文，僅鎖定「醫療機構」來強化安全措施，雖然不若HIPAA那樣複雜，但還是保有HIPAA相關的概念與意涵。

有關於「醫療資訊安全與隱私保護指導綱領草案」的九項原則包括：
1. 最小需求原則：當醫療機構或醫事相關人員蒐集、使用或揭露醫療資訊時，向另一醫療機構或醫事相關人員要求醫療資訊時，該醫療機構或該醫事相關人員必須做合理之努力，將蒐集、使用或揭露醫療資訊的範圍降至最低限度。

2. 直接取得原則：醫療機構或醫事相關人員蒐集醫療資訊時，必須直接向病人或其法定代理人為之。

3. 尊重及告知原則：醫療機構或醫事相關人員於蒐集、使用或揭露醫療資訊前，必須在尊重病人或其法定代理人，及其知情、自願的情形下為之。

4. 公平正義原則：醫療機構或醫事相關人員不可以採用非法或不公正的方法蒐集、使用或揭露醫療資訊。

5. 符合現行法規原則：醫療機構或醫事相關人員於蒐集、製作、使用或揭露醫療資訊時，都必須符合現行相關法規之規範。

6. 合理範圍內之最大安全原則：保存醫療資訊之醫療機構必須在合理的情況下，盡最大努力保護醫療資

訊之安全。

7. 病人權利保障原則：醫療機構或醫事相關人員蒐集、製作、使用或揭露醫療資訊時，必須保障病人之相關權利；而且病人對保存於醫療機構之個人醫療資訊仍享有一定之權利。

8. 不可揭露原則：醫療機構或醫事相關人員未經病人同意不得揭露醫療資訊。

9. 生命權及公共利益保障原則：病人提供以及醫療機構或醫事相關人員蒐集、使用或揭露醫療資訊時，都應以保障生命權及公共利益為原則。

儘管我們可以看到在此草案中，有許多規範，其中也有符合台灣實際醫療現況所擬的條文，但還是有人質疑，許多草案到後來通常是不了了之，「醫療資訊安全與隱私保護指導綱領草案」是否也會面臨此種狀況？台北醫學大學醫務管理系助理教授楊哲銘認為，基於電子病歷是未來的潮流，就會帶動「醫療資訊安全與隱私保護指導綱領草案」的修正。但是「醫療資訊安全與隱私保護指導綱領草案」一旦通過，對醫療機構的影響就會非常明顯，主要也是在於支出成本與作業流程方面（徐國祥，民94）。

我國的「醫療資訊安全與隱私保護指導綱領草案」要通過立法還需要很漫長的時間，楊哲銘建議，可由立法院強制立法或由衛生署訂定特別法來執行，才能夠有效保障病患醫療權益。至於如何使「醫療資訊安全」的概念有效落實在社會中，讓病患及相關醫療機構取得雙贏的局面，可能得視政府如何整合資源以及排除各種障礙了。（本文出版時間：2006-11）

參考文獻

American Health Information Management Association (AHIMA). (2006). *The State of HIPAA Privacy and Security Compliance. Chicago, IL: AHIMA. Retrieved November 27, 2006, from the World Wide Web: http://www.ahima.org/emerging_issues/2006StateofHIPAACompliance.pdf*

Junnarkar, S. (2003, June 16). Law prescribes overhaul of aging system. *CNET News.*Retrieved November 6, 2006, from the World Wide Web: http://news.com.com/2030-1070-1001641.html

Rothke, B.（民94年11月4日）。 HIPAA是否會胎死腹中？ 資安人科技網。民94年11月4日，取自 http://www.isecutech.com.tw/feature/view.asp?fid=603

徐國祥（民94年7月4日）。別讓台灣醫療安全法規無疾而終。 資安人科技網。民94年7月4日，取自：http://www.isecutech.com.tw/feature/view.asp?fid=527

黃妙慧、張克章（民95年8月21日）。國內醫療機構對病患隱私權的保護：以美國健康保險可攜性與責任法案為分析。 資通安全資訊網。民95年8月21日，取自：http://ics.stpi.org.tw/

1沙賓法案（The Sarbanes-Oxley Act [SOA]）於2002年通過，它明定企業組織必須以文件記錄各項財務政策與流程，以改善財務報告的權責制度，提高製作財務報告的效率。這項法案的主要目是要加強企業管理，恢復投資人的信心。有關沙賓法案請詳見http://www.sarbanes-oxley.com/。

推薦本篇 轉寄好友 瀏覽次數 882
友善列印 分享