以 BS7799 為基礎建構整合性醫院資訊安全架構之研究

A Study of the Integrated Architecture of Hospital Information and Communication Security based on the BS7799 Standard

陳瑞甫[a] 劉忠峰[a] 蕭如淵[b]

Rai-Fu Chen, Zhong-Feng liu, Ru-Yuan Hsiao

[a] 國立中正大學資管所 [b]國立彰化師範大學資訊工程所

[a] Graduate Institute of Information Management, National Chung Cheng University

[b] Graduate Institute of Information Engineering, National Changhua University of Education

rafuchen@mis.ccu.edu.tw

摘要

隨著社會環境的變遷、全民健保的實施以及醫療院所間彼此的激烈競爭，醫療院所的經營面對前所未有的衝擊及挑戰。醫療院所為因應上述的挑戰，也紛紛導入資訊科技以期有效提升經營績效，並增加組織的競爭優勢。然而，由於大部份醫療相關的系統在開發時都缺乏良好的規劃設計，同時未能考量未來整合性、擴充性、管理性及整體安全性上的需求，因此，常常造成後續系統維護人員系統維護及管理上的困擾。此外，雖然病歷資料的數位化可有效的提升對於病患健康照護的品質，但另一方面也衍生出安全管理以及病患隱私權保護的問題。縱觀目前國內關於醫院資訊安全方面的相關研究還是相當的不足，且缺乏一個整體的安全架構設計，導致醫院組織對於各種威脅的承受度及應變能力非常的薄弱。因此，本研究的主要目的，是以英國國家標準協會(British Standard Institute, BSI)所制定之 BS7799 資訊安全規範標準規範作為本研究的基礎，同時考量現有有限資源、技術條件以及醫療產業特殊性的要求，主要針對醫療院所防毒、防駭（包含部份隱私權保護之議題）之需求，探討 BS7799 實際應用於國內醫療院所資訊安全評估作業的適用性，並依據現行學者專家所提出之安全管理機制與技術建置出一個適用於醫療機構整合性資訊安全的架構。冀望本研究之研究成果能提供實務界與學術界，醫療機構資訊安全議題上研究之參考。

關鍵詞：BS7799、資訊安全、隱私權、醫院資訊系統