ISO 27799 健康與醫療產業資訊安全管理

資安風險升高 Healthcare 產業不容忽視的管理議題

隨著物聯網和雲端的高速發展，近年針對醫院的網路攻擊事件大幅增加，所造成資料外洩的筆數高達千萬以上。能夠連上網路的裝置，包括斷層掃描、核磁共振儀器，以及胰島素輸液幫浦等，都可能存在被入侵的風險；國內也發生過醫院的診療推車中了勒索病毒的情況。顯示資訊安全已經成為邁向高度資訊化的健康醫療產業所不能忽視的重要課題。[1]建立資安管控機制是實務上可行的對策，ISO 27799:2016 國際標準則提供了可供參考的最佳實務架構。

ISO 27799:2016 標準是關於？

ISO 27799 提供了如何保護個人健康資訊的指引，包含維持其機密性、完整性、可稽核性和可用性，不論資訊形式如何、其儲存方式，及以何種方式傳輸。這對維護病患隱私和安全非常重要。另外，醫療健康照護通常都有時效性，因此健康與醫療資訊系統在面對天然災害、系統故障和阻斷服務攻擊（denial-of-service attacks, DoS）時仍然可以運行是非常重要的。

誰會需要這個標準？

- 健康與醫療資訊安全的負責人
- 醫療健康機構
- 其他個人健康與醫療資訊的保管人
- 安全顧問
- 其他相關的顧問、稽核員和供應商
- 第三方服務提供者

為何要使用這個標準？

[1] 花俊傑（2017）。「醫療產業網路攻擊激增 循國際標準管控資安風險」，網管人，http://www.netadmin.com.tw/article_content.aspx?sn=1707070009

本標準是對 ISO/IEC 27002 標準的補充，並應與 ISO/IEC 27002 搭配使用。BS EN ISO 27799 使 ISO/IEC 27002 可以適用於醫療健康產業。它解決了醫療健康領域特有的資訊安全管理需求及其特定的運作環境。使用 BS EN ISO 27799 將有助於確保醫療健康領域：

- 維持所處理資料的機密性和完整性
- 維持關鍵健康與醫療資訊系統的運作
- 支持健康與醫療資訊的當責。此外，對於導入此標準的醫療或健康機構而言，可預期安全事件的數量和嚴重程度將會降低，員工士氣會提高，同時公眾對維護其個人健康資訊的系統也會更加信任。

健康與醫療資訊往往需要更嚴謹的保護，此標準提供了清晰、簡潔和具體針對醫療健康產業的指引，讓不論是在何地點、以何種方式提供的服務，其相關醫療健康資訊都能獲得妥善的保護。此標準並以健康資訊安全負責人員容易理解和採用的形式，提供了更多適用於醫療健康產業的要求和指引。●

深入了解 ISO 27799

1. 購買 ISO 27799:2016 標準
2. 閱讀系列文章〈**參照實施 ISO 27799 標準　強化醫療資訊安全控制**〉
   1) 醫療業資安管控第一步　從政策、組織、人員開始 – 標準第 5~7 章
   2) 清查醫療資訊相關資產　落實使用者存取控制 – 標準第 8 章~9.2.6
   3) 確保實體設施環境安全　妥善管控醫療資訊存取 – 標準 9.3.1~12.3.1
   4) 醫療記錄存取傳輸應監控　系統開發廠商妥為管理 – 標準 12.4.1~第 13 章

   ※ 以上文章出自《網管人》，由 BSI 花俊傑客戶經理撰文
3. 參加課程：ISO 27799 健康醫療資安管理指引基礎課程

請洽 BSI 訓練學苑 02-26560333#133 蕭小姐 training.taiwan@bsigroup.com

● **洽詢 BSI** ｜ 稽核驗證、產品測試、BSI 訓練學苑、VerifEye 認證平台、BSOL 標準資料庫