

醫療器材網路安全

保障病人及其醫療相關數據的安全

醫療器材與電腦網路的連結日益增加，而科技的融合暴露出裝置與軟體應用的弱點及遭至意外的可能性。保護病人資料免於受到網路攻擊，已經廣受認同。然而，對於臨床照護與病人安全的潛在影響，仍然是醫療照護組織、法規人員以及醫療器材製造商日益關切的議題。醫療器材的控管亦可能因遭到入侵而受影響。

BSI 的《醫療器材網路安全》白皮書關注於醫療保健產業因科技的融合、高度的連結以及法規的近期發展，而面臨的網路安全之挑戰。其中說明了有關安全與防護的議題與壓力，以及解決這些問題的方法。此白皮書的重點在於製造商為改善醫療器材整個生命週期的安全性，可以採取的優良作業與方法。此白皮書也有益於該產業的其他業者，包括醫療保健服務的提供者、資訊技術的供應者、驗證機構以及法規制定者。他們將明確地了解在產品整個生命週期中處理安全議題的相關規定，包括設計、採購、監控/稽核以及營運期間，尤其是當不可避免的網路意外事件發生時。

醫療器材的類別有大幅度的成長，並且往往與使用醫療應用軟體的智慧裝置連結，例如手機、平板電腦以及穿戴裝置。這些裝置已在一般家庭中存在。醫療器材固有的安全隱憂，是裝置內的資料與裝置本身的控制權都可能暴露於威脅下。這會引發安全與防護之間的拉鋸，需要所有利害關係人共同因應，尤其是透過設計與法規的方式。目前利害關係人包括法規人員、裝置的製造商、醫療照護組織、資訊科技供應商以及病人本身。

隨著醫療照護組織與消費者增加對物聯網的運用，風險勢必會增加。網路運算技術與軟體的融合，提升了醫療事業系統/資訊科技，臨床工程以及運用遠端連結之供應商的整合。但這一切將因雲端服務，以及大數據的運用，而產生革命性的變化。

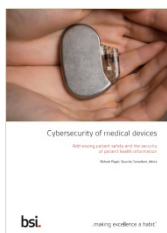
資訊科技 (IT) 以及消費性電子產品 (CE) 正借助網路而獲得橋結，由於利害關係人之間的溝通不良、傳統式的技術、安全的弱點，與裝置管理不足等因素，暴露並加劇了網路安全的弱點。醫療器材工程的重心，在於醫療安全而得以防護病人，然而儘管時有創新，但網路安全仍然不足。事實上，技術的融合引發了嶄新的攻擊通路，新技術的應用引發了網路安全的風險，雖然舊有的醫療器材仍然持續使用，但這些往往既不安全而且管理不良。雖然連結性的增加、無線網路的技術，以及超連結 (hyper-connectivity)

持續為服務的傳遞、遠端監控以及診療開創新的機會，但是也可能引發出無法預期的結果。由於潛在敵人透過網路攻擊而導致的網路意外事件，也大幅地增加。

除了許多重大的意外事件，醫療器材安全已經成為醫療照護安全的首要問題。無疑地，提供一個被惡意軟體侵入的裝置，有可能毀壞醫院的運作，洩露重要的病人資料、損及其他連結裝置，並且損害到病人。

針對日益增加的網路安全威脅之處理的新方法，建議所有相關者，確認並且評估網路風險與威脅、針對意外事件規劃降低風險，並且採取適當的回應模式，以確保病人的安全與防護。

許多醫療器材指南都是近期且持續發展中。無論是從技術的觀點，或是醫療照護利害關係人之間都有所整合，並認識到網路安全需要各方的合作。探討醫療器材風險的重心，一般著重於功能的安全、安全相關的風險（不包括網路安全），或是數據保護；目前已有許多方法正在積極應對網路安全事件衍伸出的生命週期風險和潛在危害。醫療器材製造商可採取網路安全成熟度評鑑，確認並排出改進作業的優先領域。其中應該包括產品生命週期安全，訂定出評估的架構，並且列在醫療照護內容之中。完備的意外事件回應計畫與作業流程，對於醫療照護事業體，預先因應無法避免的網路安全事件是非常重要的。●



《醫療器材網路安全》白皮書

這份由 BSI 發布的白皮書，內容涵蓋了與病人及其醫療數據安全相關的網路安全基本概念，並評估使用透過網路連結的醫療器材可能的風險及挑戰。此外並介紹了美國和歐盟有關網路安全的規定。[下載白皮書請按此>](#)

BSI 資訊安全系列課程



資訊安全管理 ISO 27001

學習最標準且完整的風險分析及處理程序，協助組織建立一套完整的資安管理系統，有效解決當前資安問題，並降低日後資安管理可能面臨的風險。[課程詳情>](#)



個人資訊管理 BS 10012

學習個資管理實務上的 PDCA 作法，及運用這套架構來開發、建置和審視組織的個資管理工作，協助您符合主管機關的規範，還能做到持續改善的有效管理。[課程詳情>](#)



雲端服務資安暨個資保護 ISO 27017+ISO 27018

雲端服務的適法性和安全性一直是使用雲端服務的企業要面對的重要課題，本課程協助學員具備充分的知識及技能，促使企業達到雲端服務上個人資料保護及資訊安全管理的目的。[課程詳情>](#)