數位健康大未來 系列報導 2
台灣醫院個人資料安全保護新規範

生技醫療服務團隊

Contact us
+886 2 27296666 #21991
bioservice@pwc.com

執業會計師：

生醫產業負責人
林玉寬 Amenda Lin #35105
周筱姿 Zoe Chou #26683

醫藥醫材
游淑芬 Jasmine Yu #26138
鄧聖偉 David Teng #26123
王玉娟 Jane Wang #40168
田中玉 Chung-Yu Tien #60106
劉倩瑜 Chien-Yu Liu #35323

醫療照護
蔡晏潭 Yen-Tan Tsai #26997
馮敏娟 Jackie Feng #26609
林雅慧 Anny Lin #26816

生技新創
廖阿甚 A-Shen Liao #25128
江采燕 Tsai-Yen Chiang #35381
顏裕芳 Yu-Fun Yen #25489
吳偉豪 Kenny Wu #34306

財務顧問
翁麗俐 Lily Wong #26703

稅務服務
黃文利 Jack Hwang #26061

法律服務
楊敬先 Ross Yang #26100

副總經理：
項益容 Jessica Hsiang #21990

數位健康新時代正在來臨，個人資料如病歷和醫療個資等蒐集、處理、利用或跨單位傳輸分享將成新常態，並藉數據分析獲得更好的醫療服務，然資料安全議題亦隨而浮現，世界經濟論壇更早在 2017 年就將資安列為全球五大風險之一。

根據資誠數位健康產業調查顯示，台灣生醫領域在資安意識仍有努力空間，而保存大量的病歷或就醫個人資料的醫院更是資安攻擊重要目標。台灣衛福部於 2020 年 7 月 10 日公告《醫院個人資料檔案安全維護計畫實施辦法》，隨著該辦法將於 2021 年 1 月 10 日正式生效施行，醫院如何提早準備並擬定資料安全維護計畫刻不容緩。

敲響資訊安全警鐘

數位時代下，民眾對於個人資料(以下簡稱個資)保護之需求日增，如何確保個資安全維護，避免個資遭受盜用或濫用，不僅持續受到民眾重視，亦是保存個人資料的單位須要謹慎面對的重要議題。

根據資誠《數位健康大未來》[註 1] 產業調查顯示，台灣生醫領域在資安保護意識仍有努力的空間，除企業宜即早遵循國內外個資管理規範，構思資安風險管理策略外，保存大量醫療個資的醫院恐怕也無法置身事外，以橫掃全球的 WannaCry 勒索病毒攻擊為例，該病毒攻擊癱瘓英國國家健保局（National Health Service, NHS）旗下的

數位健康大未來 系列報導 2
台灣醫院個人資料安全保護新規範

多家醫院醫療資訊系統，使得超過 19,000 例的預約看診和手術被迫取消[註2]，急需手術治療或醫療照護的民眾因此無法得到適當診療，造成相當程度的健康損失；而台灣多家醫院也無法倖免，敲響資訊安全警鐘。

醫院保存大量民眾醫療個資 資安維護更為重要

作為提供民眾醫療照護服務的醫院，從民眾掛號、問診看診，乃至於抽血、檢體或醫學影像檢查、手術治療以及用藥等過程，皆涉及民眾大量醫療個資之蒐集與處理，而這些醫療個資都將保存於醫院資訊系統，駭客藉由入侵、竄改、毀損、惡意加密，將造成醫師誤用醫療個資或遭拒用（無法使用）而提供錯誤的診療處置，間接違害民眾的健康。

醫院個人資料檔案安全維護計畫實施辦法重點說明

為加強醫院對於個人資料之保護，維護資料安全性，衛生福利部醫事司於 2020 年 7 月 10 日公告《醫院個人資料檔案安全維護計畫實施辦法》[註3]（以下簡稱實施辦法），防止醫院內的個人資料被竊取、竄改、毀損、滅失或洩漏，該實施辦法將於 2021 年 1 月 10 日正式生效施行。

該實施辦法依循台灣《個人資料保護法》[註4]（以下簡稱個資法）之規範原則，共計有 20 條條文，其明定醫院須訂定安全維護計畫，落實在個人資料蒐集、處理及利用等階段，以及業務之特定目的終止或期間屆滿後的完整保護，保障民眾就醫安全性。

解讀本實施辦法可以發現，醫院在個人資料之蒐集、處理及利用上，例如: 需符合特定目的與必要性、界定個人資料類別或範圍、蒐集前的告知義務等，皆依循現行《個資法》規範。然醫院則須依循本實施辦法，建立起管理、應變、稽核以及改善機制，內容整理詳如下表 1。其重點包括：

首先，醫院應建立接觸個資人員以及資料之管理機制，如制定接觸個資人員權限、分層管理、以及持續教育訓練增進人員的資安意識；並針對資料檔案的保存、紀錄、轉移、設備加密以及業務終止後的資料檔案刪除訂定明確規範。

其次，醫院應考量可能的風險事件發生制定應變機制，如採取適當措施，盡可能在事前進行事故控制、事中的查明事故原因與通報機制、以及事後的改善措施，避免同類事故再次發生。

再者，醫院應透過指定相關人員以定期稽核、持續檢討以改善個人資料檔案的安全維護。

此外，醫院如委託他人進行全部或一部分之個人資料之蒐集、處理

或利用時，應對受託人進行適當監督，並於委託契約或相關文件中明確約定。

表 1、醫院個人資料檔案安全維護計畫實施辦法重點說明

機制		說明
管理	人員管理	制定接觸個資人員（所屬人員）管理機制 • **設定權限：** 對醫院內接觸個資人員（所屬人員）**設定權限**，管控其接觸個資，並定期確認權限必要性與適當性 • **分層規範：** 依業務性質規範相關負責人員 • **保管保密：** 要求所屬人員妥善保管個資之儲存媒介物，並**約定保管及保密義務** • **終止權限：** 終止所屬人員離職後之權限，要求辦理交接，並**不得攜離使用** • **教育訓練：** 所屬人員應明瞭個資法相關規定、範圍、及應遵守措施
	資料管理	• **資料檔案保存：** 1. 紙本資料檔案應設置**安全保護與管理程序** 2. 電子資料檔案存放之設備應配置安全防護系統或加密機制，並應**設置備份機制** • **資料檔案紀錄：** 個人資料使用紀錄、設備之軌跡資料或其他相關證據資料**應至少留存6個月** • **資料檔案轉移：** 保存資料之儲存媒介物（如紙本或設備）若有報廢、汰換或轉作其他用途，應**確保資料檔案完全移除**，避免外洩 • **資料檔案刪除：** 醫院業務終止時，宜將保有之個人資料進行銷毀、移轉或其他刪除、停止處理或利用，並製作成紀錄，且**應至少留存5年**
應變		• **事前應變：** 採取適當措施，控制事故對於當事人造成的損害 • **事中應變：** 查明事故原因及損害狀況，以適當方式通知當事人，並通報主管機關 • **事後應變：** 研議改善措施，避免事故再度發生
稽核		• **定期稽核：** 醫院應指定查核人員，負責**每年評核**安全維護計畫之執行成效，並向醫院提出報告，持續修正
改善		• **持續改善：** 醫院應指定專責人員負責規劃、訂定、修正及執行資料安全維護計畫，依執行狀況持續修正改善

資料來源: 衛生福利部，資誠整理(2020/08)

數位健康大未來 系列報導 2
台灣醫院個人資料安全保護新規範

結語

台灣在全民健保實行、醫療資訊化與電子病歷推動計畫下，全台 22,992 家醫院[註 5] 所保存的大量民眾病歷與醫療個資成為台灣發展數位健康優勢，然這些數據金礦卻也容易成為駭客攻擊的目標，資安保護成為重中之重。

資安是一場永不完結的攻防戰役，正所謂「知彼知己，百戰不殆」，駭客經常使用的策略就是找出資安弱點並加以利用。為此，醫院應通盤思考合理的資安策略，從資料在蒐集、處理及利用之完整流程中找出機構內可能的資安破口，而人員、資料管理、設備等都有可能是潛在的資安漏洞，醫院宜盡早依循本實施辦法建立管理機制，並定期追蹤與持續修正，完善個人資料安全維護。

隨著物聯網與 5G 的快速進展，健康或醫療個資的跨單位或跨國傳輸將成新常態，台灣醫院或企業除滿足國內規範外，如何通盤考量國際規範並加以因應亦是重要議題。觀察主要國家如美國或歐盟等在個資保護皆訂有相關規範，而其中與台灣個資規範則略有不同，將於下篇內容進行分析與探討，敬請期待。

資誠生醫透視長期關注台灣生醫產業發展，將持續針對數位健康發展發布系列報導，敬請期待。如欲知《數位健康大未來》報告重要內容，亦歡迎造訪資誠網頁。

數位健康大未來 系列報導 2
台灣醫院個人資料安全保護新規範

參考資料

1. 資誠聯合會計師事務所（PwC Taiwan），數位健康大未來，2020 年 7 月。
   https://www.pwc.tw/zh/publications/topic-bio/digital-health.html
2. The Telegraph, “WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled,” Oct, 2018.
   https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/
3. 衛生福利部，醫院個人資料檔案安全維護計畫實施辦法，2020 年 7 月。
   https://gazette.nat.gov.tw/egFront/detail.do?metaid=116946&log=detailLog
4. 國家發展委員會，個人資料保護法，2015 年 12 月。
   https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021
5. 衛生福利部，醫療院所家數、病床數及平均每萬人口病床數，2020 年 6 月。
   https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

周筱姿 會計師
Zoe Chou

☎ (02) 27296666 #26683
✉ zoe.chou@pwc.com

| 現任・經歷 |

- 資誠生醫產業負責人
- 資誠聯合會計師事務所會計師
- 衛福部 107 年度「長照機構法人財報編準草案研究」協同主持人
- 財團法人資誠教育基金會專案督導
- 資誠 Global Government and Public Services 產業負責會計師
- 專書《公益理想實踐之路：非營利組織之設立與管理實務》共同作者

| 專長 |

- 公開發行及上市櫃之規劃及輔導
- 生技及高科技產業、公益及醫療財團法人之顧問諮詢及查核
- 輔導或查核國內多家生醫企業與 10 餘家大型財團法人