數位健康大未來 系列報導 3
健康相關資料使用與保護關鍵議題

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
劉美蘭 Mei-Lan Liu #40188
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

併購與財務顧問
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，個人資料如醫療數據等之蒐集、處理、利用或跨單位傳輸分享將成新常態，並藉由數據分析獲得更好的健康與醫療服務，而過程中卻伴隨個人隱私安全的問題。

健康相關數據資料多源自於個人，美國與歐盟皆訂定個人資料保護相關規範，然台灣健保制度推行了 30 多年，擁有發展數位健康的資料金礦，國家發展委員會於 2019 年啟動個人資料保護法之修法作業，如何權衡促進健康大數據之產業利用與民眾個人資料保護權利，實為政府推動數位健康產業政策關鍵議題。

數據隱私安全為數位健康發展關鍵議題

數位健康新時代正在來臨，打破傳統醫療服務在空間與時間藩籬，而數位科技如穿戴裝置、軟體應用程式、5G 行動通訊技術、醫療物聯網設備等推陳出新，大幅便利民眾在健康相關數據的量測與蒐集，使民眾更願意使用並分享數據，以獲得更佳的健康與醫療服務。

然健康相關數據勢必涉及個人敏感資訊，大多數民眾更認為其屬於隱私且應當受到保護，根據國際管理顧問公司 Accenture 2019 年研究調查指出，高達 92%受訪民眾表示，確保數據隱私安全是重要或極度重要的。

台灣雖然以《個人資料保護法》為主要法規依據，但資料能否提供

數位健康大未來 系列報導 3
健康相關資料使用與保護關鍵議題

產業運用上仍面臨諸多討論與挑戰[1、2]，例如健康相關資料去識別化程度到如何才可提供產業運用？而健康相關資料二次利用限制「學術研究」等適用範圍，使得後續商業運用受到限制等。觀察主要國家如美國與歐盟等在保護個人資料的蒐集、處理與利用，在適當保護與限制的前提下，雖兩者之規範不同，但整體而言，得以令台灣產業運用數據以發展數位健康創新解決方案的思維值得借鏡。

以下將針對主要國家美國與歐盟在個人資料使用與保護之規範與要點進行說明與分析比較。

美國：健康保險可攜性與責任法(HIPAA)

美國在個人隱私安全保護可追溯至 1974 年的《隱私權法(The Privacy Act)》，該法規範政府機構於美國公民個人數據之蒐集、使用與處理。

而 1996 年通過《健康保險可攜性與責任法(Health Insurance Portability and Accountability Act，HIPAA)》是針對專門為「**個人健康資訊**」訂出的規範法律，並賦予民眾對自身健康資訊的權利，隨後並與時俱進針對該法之授權子法不定時修改補充，完善在個人健康數據隱私與安全保護。

該法明訂個人健康資訊(Protected Health Information，PHI)保護範

圍，並定義何種適用主體（即何者或何種團體和機構）可以查看、蒐集、處理與使用個人健康資訊；以及適用主體如何建立資料安全保護措施。

HIPAA 藉由設立專家決定機制(Expert determination)與安全港機制(Safe Harbor)，確保 PHI 去識別化後無法識別出個別健康資訊，可提供第三方作為產業利用，值得台灣借鏡。

以下就 HIPAA 重點說明詳如下表 1：

表 1、美國 HIPAA 重點說明

項目	內容
適用數據類型 (受規範之數據類型)	• **受保護的健康資訊(Protected Health Information, PHI)**指可識別出個人的健康資訊，如病歷紀錄、健保號碼等；無論是口頭、書面、電子或媒體儲存等形式
適用主體 (受規範單位)	• **服務提供業者**，如醫療機構或醫師 • **健康計畫管理與給付單位**，如保險機構 • **數據處理分析公司** • 以及向上述單位提供服務之**商業夥伴**，如提供雲端儲存或服務業者
適用主體義務	適用主體應具備合理的資訊安全保護措施，可分為： • **行政管理**安全維護 • **物理性**之安全維護 • **資訊技術**安全維護
資料主體權利 (即民眾個人)	• **知情同意權**：適用主體使用PHI前須經民眾個人知情與同意，而部分特殊情形得以例外[註1] • **限制使用權**：民眾個人可對自己PHI進行使用權限之限制 • **申請獲取權**：民眾個人可向適用主體申請取得其儲存的所有PHI • **修改權**：民眾個人可要求適用主體修改其錯誤的PHI • 使用紀錄知情權：民眾個人可向適用主題要求近 6 年的使用紀錄
風險通報	• 適用主體如發現可能危害資料主體之風險事件，如資料外洩，**必須於60天內**通知當事人(資料主體)。 • 若風險事件受波及人數超過500人，則必須同時即時通報美國衛生及公共服務部(HHS)；若為受波及人數未達500人，可於當年度結束60天內與其他事件合併項HHS申報
其他	• **數據利用**：適用主體可將經去識別化(de-identification)的PHI提供第三方進行產業利用，而去識別化的PHI須符合安全港機制[註2]與專家決定機制[註3]。

註 1：例外情形如: (1)提供治療、支付/給付或與醫療行政管理(Health Care Operations)之目的；(2)有特地法律之規定者；(3)基於其他被允許行為之意外使用或揭露；(4)公共利益有關之目的；(5)基於研究、公共衛生或健康照護之目的等。

註 2：安全港機制指須將移除可識別出個人的 18 項關鍵數據，分別為(1)姓名、(2)地址(小於州之資訊，如街道、城市、地區和郵遞區號等)、(3)除年份以外與個人相關的日期資訊(如生日、入院日期、出院日期、死亡日期等)、(4)電話號碼、(5)傳真號碼、(6)電子郵件、(7)社會安全號碼、(8)病歷編號、(9)醫療保險號碼、(10)銀行帳號、(11)證件號碼(如身分證、駕照等)、(12)車輛登記號碼(含車牌號碼)、(13)醫材標示號和序列號碼、(14)網際網路標準位址(Web URL)、(15)網際網路協定位址(IP Address)、(16)指紋或聲音等生物標記資訊、(17)個人照片、(18)任何其他可用於識別的編碼或特徵資訊。

註 3：專家決定機制由統計專家或行業具經驗的專家決定哪些關鍵數據必須刪除，並提供評估分析結果

資料來源: 美國衛生及公共服務部，資誠整理(2020/11)

歐盟: 一般資料保護規範(GDPR)

歐盟 1995 年的《數據保護指引(Data Protection Directive)》為會員國在規範個人資料保護的參考依據。隨著資通訊科技進展，原指引已不合時宜，歐盟啟動修法，於 2016 年公告《一般資料保護規範(General Data Protection Reregulation, GDPR)》，並於 2018 年 5 月生效，將原先之指引(Directive)升級至法規(Regulation)層級。

GDPR 賦予資料主體更大權利，有權了解適用主體如何利用自動化決策(如大數據、人工智慧等)進行處理且亦有權拒絕；同時亦擴大適用主體的約束範圍，除設立於歐盟的數據處理機構外，亦約束設立於歐盟境外但處理歐盟資料主體之機構單位。GDPR 重點詳細說明可參考下表 2 所列。

表 2、歐盟 GDPR 重點說明

項目	內容
適用數據類型 (受規範之數據類型)	• **一般個資**: 得以直接或間接方式識別個人之任何資訊，如姓名、電話號碼、地址以及數位資料（網路識別碼、行動裝置ID）等 • **特種個資**: 如個人基因資料、可識別個人之生物特徵數據（如種族、血統、遺傳疾病、健康相關資料等）、政治意見、宗教等
適用主體 (受規範單位)	• **設立於歐盟境內**，涉及資料處理管控者(Data Controller)以及受託處理資料之資料處理者(Data Processors) • **設立於歐盟以外，但對處理歐盟境內居民個資、或提供商品服務**之資料管控者與資料處理者
適用主體義務	• **個資保護之設計(by design)與預設(by default)機制**：運用科技以及組織的相關措施，以保護個資，如採取假名化或匿名化等加密技術保護個資、數據系統監控風險能力、因應風險事件的評估與測試，事故發生後的回覆程度等，確保一定程度的安全性。 • 如涉及大規模的數據監控或涉及健康相關資料處理者，應於事前進行**數據保護影響評估**，評估為高風險者須事前諮詢監管機關。
資料主體權利 (即民眾個人)	• **訪問權**：民眾有權查看自己的個人資料、處理狀態、處理目的和正在處理的數據類型 • **更正權**：有權要求更正不正確個資，且有權補充個資 • **刪除權**：與原先處理目的不同、處理目的消失或違法處理時，有權要求刪除及停止使用，並撤回同意 • **可攜帶權**：有權要求個資由一個管控者移轉或傳送至其他管控者 • **限制處理權**：有權要求限制處理 • **拒絕權**: 有權拒絕適用主體處理個資之方式；以及有權了解特定服務是如何利用自動化決策(如大數據、人工智慧等)進行處理，並有權拒絕於類似分析
風險通報	• 風險事件發生後應主動與當事人聯繫並說明侵害情形，同時應於事件發生**72小時內向**監管機關通報 • 如涉及大規模數據管控或處理，或需要處理大規模的基因資料、生物特徵資料或健康資料等特種個資者，應指定專業資格的數據保護長(Data Protection Officer)
其他	• **健康相關數據利用**：原則禁止處理與個人健康相關資料[註1]，**然例外情形[註2]得以為之**。 • **資料二次利用**：原則禁止資料二次利用[註2]，然**例外情形得以為之**[註3]，如用於科學研究之目的，其中私人贊助研究符合科學研究之範圍。 • **資料跨境傳輸**：原則上禁止資料跨境傳輸，然例外情形得以為之[註5]。：

註 1：GDPR 禁止處理如基因資料、用以識別自然人之生物特徵識別資料、或與健康相關等特種個資。

註 2：得以處理個人健康相關資料之例外情形為「當事人表示明確同意(第 a 項規範)」、或「用於處理預防或職業醫學、醫學診斷、健康照護系統和服務之管理(第 h 項規範)」、或「該處理係於公共衛生領域基於公益理由，如用於防範跨境之健康重大威脅」，或「用於為醫療保健、醫療產品或醫療設備之高品質與安全標準者，並已依歐盟法或會員國法令採行維護當事權利及自由之適當特殊措施，而認有必要者(第 i 項規範)」。

註 3：GDPR 第 5 條明定資料蒐集目的特定、明確及合法，且不得為該等目的以外之後續處理(二次利用)，

註 4：GDPR 第 89 條第 1 項說明資料得以二次利用之情形，如為達成公共利益之目的、科學研究(Scientific Research)目的或歷史研究目的或統計目的所為之進階處理，不應視為不符合原始目的。

註 5：資料可跨境傳輸之例外情形，如第三國取得歐盟委員會適足性認定、機構/企業自行採取符合規範的保護措施、或經資料主體明確同意等其他例外情形。

資料來源: 歐盟議會，資誠整理(2020/11)

值得台灣借鏡的是，GDPR 強化適用主體責任義務，如涉及大規模的數據監控或涉及健康相關資料處理者，應於事前進行數據保護影響評估(Data Protection Impact Assessment)，並事前諮詢監管機構。

此外，在 GDPR 資料目的原則下，雖不得為該目的以外之後續處理，但為達成公共利益之目的、科學研究(Scientific Research)目的或歷史研究目的或統計目的所為之進階處理，則允許資料二次利用。其中，對於科學研究目的之定義則採取寬鬆解釋(Broad Manner)，如私人贊助研究(Privately fund research)皆符合科學研究之範圍。

結語與建議

美國 HIPAA 雖早於 1996 年推出，過程中持續因時制宜修訂，如將商業夥伴(如雲端儲存或服務業者)納入規範；同時透過安全港機制與專家決定機制支持，使產業得以利用，即凡經去識別化的 PHI 可提供第三方進行產業利用。

觀察台灣個資法立法內容與歐盟 GDPR 較為相近，部分條文與規範範圍更有異曲同工之精神，然而在健康相關資料的二次利用之適

用範圍則有所不同。如台灣個資法在資料二次利用限於**學術研究而有必要**等範圍，然歐盟 GDPR 之**科學研究包含私人贊助的研究**，其適用範圍更加寬廣；此外，在國際傳輸方面，台灣現行則採取「原則許可，但例外禁止」之規範，與歐盟 GDPR 之「原則禁止，但例外許可」精神則有所不同。

以長年累積的健保資料庫、人體生物資料庫等健康大數據為根基，台灣擁有發展數位健康的資料金礦，如何權衡促進健康大數據之產業利用與民眾個人資料保護權利，並盡可能取得平衡，成為政府推動數位健康產業不可避免的重要關鍵。

為此，國家發展委員會已於 2019 年啟動個人資料保護法之修法作業。基於大幅修改法條之成本與民情意見的考量，或許無法如同美國 HIPAA 將經去識別化的個人健康資料直接提供給產業利用，惟建議可參考歐盟 GDPR 在資料產業利用之精神，如將資料二次利用適用範圍由目前學術研究調整為科學研究，並建立相關配套措施，在保障民眾權利下得以讓產業進行利用；同時調整國際傳輸規範，強化台灣數據保護力，實為可以思考的關鍵議題。

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。

pwc 資誠

數位健康大未來 系列報導 3
健康相關資料使用與保護關鍵議題

參考資料

1. 工商時報，「解放醫療大數據 發展智慧健康產業」，2017 年 5 月。
   https://www.chinatimes.com/newspapers/20170518000072-260202?chdtv
2. 監察院新聞發布，衛福部健保資料庫管理及運用爭議，2020 年 7 月。
   https://www.cy.gov.tw/News_Content.aspx?n=640&s=18146
3. 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
4. 美國衛生及公共服務部，健康保險可攜性與責任法(HIPAA)
   https://www.hhs.gov/hipaa/index.html
5. 歐盟議會，一般資料保護規範(GDPR)
   https://gdpr-info.eu/
6. 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
7. 國家發展委員會，個人資料保護法施行細則，2016 年 3 月。
   https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050022

作者介紹

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合夥會計師
- 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
- 教育部護校改制護專審查蹤訪視委員會委員
- 教育部生醫產業與新農業跨領域人才培訓計畫委員
- 資誠 Global Government and Public Services 產業負責會計師

| 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
- 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