財團法人醫藥品查驗中心 Center for Drug Evaluation, Taiwan 當代醫藥法規月刊 2018-06-08 92
回 CDE 官網首頁
訂閱/取消電子報

個人健康醫療資訊之美國與歐盟法規管理方向

葉錫誼[1]

前言

追求個人化醫療是醫學發展的終極目標。近數十年，隨著人類基因體的研究，已使標靶藥物之精準醫學有長足的進步。而物聯網及人工智慧技術的發展，除了生理訊號及基因表現等特徵外，包括過往病史、生活習慣等更廣泛的個人健康醫療資訊之儲存、收集、監測與分析研究，也逐漸成為新醫療照護技術發展的重要方向。依 TrendForce 網站發布之報告，2017 年參與德國 Dusseldorf MEDICA 全球醫療器材大展的廠商中，所有能產出「臨床醫療數據」的醫療器材，幾乎都已具有與雲端資料庫或遠端數據中心連結溝通的能力，縱使暫時無法與雲端串連，也都設計了數據轉出的功能；除了常見生理資訊記錄之外，亦包含各種專業醫療檢測、監控設備之間的聯動、醫療數位服務平台等。顯示數位應用的能力，已在臨床醫療領域中普及運用，醫療器材數位化、雲端化的時代已正式來臨[1]。

然而，近年來持續發生的各種資訊安全事件，也引起大眾對網路與資訊系統安全之疑慮，例如 2017 年 5 月份爆發的「WannaCry」惡意軟體勒索攻擊，曾造成全球 1 百多個國家受害，政府單位、企業、醫療、高校等各行各業都受到影響，甚至連英國的醫療系統都一度面臨服務癱瘓的威脅，使部分常規手術被迫臨時取消[2,3]。又如近期經媒體報導曝光的不法數據公司，利用心理測驗應用程式，違法蒐集取得臉書社群平台逾 8700 萬筆的用戶個人資料，並藉以進行不法分析[4]，亦突顯個人資料管理的重要。面對持續升高的資安威脅，本文將針對美國與歐盟近年著手進行之個人健康資訊管理，其法規要求及發展方向予以介紹。

美國之個人健康資訊管理相關法規

[1] 財團法人醫藥品查驗中心醫療器材組

一、法源依據與適用範圍

美國聯邦政府於 1996 年即已頒佈「醫療保險可攜與責任法案(Health Insurance Portability and Accountability Act, HIPAA Act)」，授權衛生及公共服務部(Department of Human and Health Services, HHS)制定個人健康醫療資訊相關規範，其中 2002 年發布的隱私規則(Privacy rule)與資安規則(Security Rule)，即成為美國對個人健康資訊管理的主要架構[5,6]。2009 年為進一步推動電子病歷應用而制定的「經濟和臨床健康之健康資訊科技法（Health Information Technology for Economic and Clinical Health Act, HITECH Act）」[7]，則強化資料外洩時相關機構的通報責任與違反 HIPAA Act 的處罰，並於 2013 年整合修訂為 HIPAA 最終規則(HIPAA final omnibus Rules)[8]。

在 HIPAA/HITECH 的架構下，包含醫療照護的提供者(Health Care Provider)、保險機構等健康計畫(Health Plan)的管理與給付單位、健康資訊處理機構(Health Care Clearinghouses)、以及向上述單位提供服務的業務夥伴(Business associates)等「受管轄機構(covered entity)」。只要涉及受保護健康資訊(Protected Health Information, PHI)都必須符合相關規範的要求。其中，受保護健康資訊在 HIPAA 隱私規則(Privacy rule)的定義下，涵蓋任何的個人可識別健康資訊(individually identifiable health information)，無論是以何種格式持有，以及包含口頭、書面、電子等任何形式的傳輸，都必須符合 HIPAA 隱私規則(Privacy rule)的要求。針對以電子格式傳輸的受保護健康資訊(e-PHI)之安全維護議題，則進一步以 HIPAA 資安規則(Security Rule)加以規範。

另一方面，如果企業涉及任何個人隱私和數據安全的洩漏與不當利用，也會被視為是美國聯邦貿易委員會法(Federal Trade Commission Act, FTC Act)第五條所規範的商業中或影響商業的不公平競爭方法或欺騙性行為，將面臨 FTC Act 的相關罰則[9]。

為進一步促進網路安全資訊的交流，美國總統歐巴馬於 2015 年簽署通過「網路安全法案(Cybersecurity Act of 2015)」[10]，除了加強美國聯邦各部門間的資安交流機制，

也將建立一個自願性的網路資訊安全分享架構，免除民間機構向公務機構提供網路安全資訊的相關法律責任，期盼藉由提高網路資安訊息共享來改善網路安全問題。然而，該分享架構也賦予私人機構監控、分享或接收資訊情報的權利，涉及對客戶個資隱私的侵犯疑慮，而引起大眾及許多企業的反彈[11]，後續的執行情形仍需要持續觀察。

二、HIPAA/HITECH Act 架構下之個人健康資訊安全保護原則與維護要求

(一) 隱私規則(Privacy Rule)

1. 原則上禁止未經授權的使用或揭露

適用 HIPAA/HITECH Act 的受管轄機構除了當事人書面授權外，不得任意使用或洩漏個人受保護健康資料，但在符合下列情形下，允許受管轄機構可在未經當事人授權下使用或揭露個人受保護健康資訊:

(1) 治療、給付與健康照護之運作；

(2) 基於其他被允許行為之意外使用或揭露

(3) 公共利益有關之活動

(4) 基於研究、公共衛生與健康照護目的提供之有限資料(Limited Data Set)

另一方面，當事人有權向受管轄機構要求使用(access)或結算(accounting)其個人受保護健康資料檔案，最多可要求提供近六年之資料。若特定的醫療處置行為完全由當事人自行負擔其費用，當事人可限制受管轄機構針對該筆醫療資料之處理。美國衛生及公共服務部(HHS)基於調查或研究所需，也可要求受管轄機構向其提供個人受保護健康資料。因此，受管轄機構所持有之個人健康資料必須保存最少六年之期限。此外，由於 HITECH Act 的修正規則中，明定禁止受管轄機構在未獲當事人同意下販售個人受保護健康資料，如果是基於研究等允許事項之目的而需提供其他單位個人受保護健康資料，

則受管轄機構僅能收取符合其準備及傳輸受保護健康資料所需成本之費用。同時，修正規則也禁止受管轄機構於行銷訊息中使用或揭露未經授權的受保護資訊，除非該訊息是描述針對個別當事人的處方藥品或生物製劑，且受管轄機構協助進行該行銷活動而獲得之報酬並未超出合理範圍。

2. 最少必要原則(Minimum Necessary)

受管轄機構僅能使用或揭露為達特定目的所需之最少且必要之個人受保護健康資料。為符合此原則，受管轄機構必須制定相關制度與評估機制，並須提供其隱私保護政策之相關說明，以達到個人受保護健康資料僅可供合理使用與揭露之法規要求。

3. 分級授權使用原則

受管轄機構必須針對其內部人員制定分級使用個人受保護健康資料的機制，依職務身分之不同，限制其能接觸使用的資料範圍。

4. 應採取之隱私保護措施

為確保個人受保護健康資料之隱私安全，HIPAA 隱私規則中明文要求受管轄機構必須制定相關之隱私保護措施，包括須制定機構內的隱私保護政策與施行步驟，並須指定 1 名負責隱私保護業務之管理人員(privacy personnel)，且需有相關的人員教育訓練與管理制度以確保制定的隱私保護政策能在機構內落實執行。此外，機構內還須針對資料安全設置適當的保護工具與技術。另一方面，為能及時獲得資料外洩之訊息，隱私規則中亦要求受管轄機構應建立一套客訴系統，並於察覺違反隱私規則之事件發生時，能盡快擬定與施行危害減輕措施。但有鑑於各個受管轄機構間，存在規模與資源之差異，因此 HIPAA Act 中並未強制要求每一個機構都必須執行所有的安全要求項目，而是賦予受管轄機構可以視其自身的條件所需，選擇性的執行經評估後認為有必要之安全措施，但必須將其評估分析過程加以記錄以說明其合理性。

(二) 資安規則(Security Rule)

1. 須確保電子資料之機密性、完整性與可取得性

HIPAA Act 的資安規則主要針對以電子檔案型式存在之個人受保護健康資料。受管轄機構於產生、接收、維持和傳輸電子健康資訊時，除了隱私規則所要求必須確保資料不得在未經授權的情況下使用或揭露以維持其機密性(confidentiality)，針對資訊安全的部分還必須確保電子資料的完整性(integrity)，不能被未經授權的修改或破壞。同時，也必須確保電子資料的可取得性(availability)，可依授權使用的目的進行傳輸或存取。為此，受管轄機構必須符合下列資訊安全維護要求：

(1) 識別並預防可合理預期的資安威脅；

(2) 預防可合理預期的未允許使用或洩漏情形；

(3) 確保旗下員工能符合資安規則的要求。

2. 應具備資訊安全維護措施

為達到上述資訊安全之目標，於 HIPAA 資安規則中明定受管轄機構必須具備合理的資訊安全維護措施，包含 A.行政管理之安全維護、B.物理性之安全維護、C.資訊技術上之安全維護等三種類型之防護方法。其中，於行政管理上，應指定 1 名機構內人員擔任資訊安全負責主管，並針對資訊安全、資料庫存取、人員教育訓練及資安威脅的評估等制定相關的管理機制。物理性之安全維護則是針對機構內的設施使用應有管控機制，工作場所及儀器設備也應有保安措施；此外，應藉由資訊科技的技術方法，例如電子資料存取的授權機制、資訊系統運作的紀錄與監測、資料完整性之維護、網路傳輸安全性之確保等以提升電子資料的安全性。當受管轄機構決定要執行哪些安全維護措施時，應將資料的規模與複雜性、該機構所具有的技術及軟硬體設施、安全維護措施的成本、潛在風險發生的可能性與其可能造成的衝擊等因素綜合納入考量。

3. 應執行風險分析與危害管控

依 HIPAA 資安規則的要求，受管轄機構應將風險分析納入資安管理程序中，並規定風險分析過程應包含但不限於下列事項：

(1) 評估潛在風險發生的可能性與造成的影響程度；

(2) 針對已鑑別風險施行合適的安全處置方法；

(3) 針對所採取的安全維護措施之合理性說明；

(4) 持續維持合宜的安全保護措施之作法；

風險分析應是一個持續不斷的過程，受管轄機構應定期檢視和追蹤電子健康資料的存取記錄，並偵測安全危害事件的發生次數，同時也應定期評估安全維護措施的有效性和可能的潛在風險以進行危害管控。當受管轄機構發生或發現其業務夥伴出現資料洩漏或違反資安規則的事件時，必須採取合理的處置方式以緩解並降低其危害程度。

(三) 發生健康資料外洩時之危害通報要求

2009 年的 HITECH 法案中，針對 HIPAA Act 的受管轄機構強化了個人受保護健康資料外洩時的通報責任。當發現可能危害當事人的未加密個人健康資料外洩時，必須於 60 天內將資料外洩情形與相關處置方法通知當事人，若資料外洩波及的人數達 500 人以上時，則必須同時及時通報美國衛生及公共服務部(HHS)。此外，若是波及的人數於某一州或特定行政區域內超過 500 人，受管轄機構還必須於 60 天內通知當地媒體。另一方面，若單一資料外洩事件的波及人數未超過 500 人，則可於當年度結束後 60 天內，與其他事件合併向 HHS 申報。

隨著提供數位健康產業服務的業者結構之多樣化發展，如果是不屬於 HIPAA/HITECH Act 受管轄機構的健康資訊外洩情形，依據美國聯邦貿易委員會(FTC)於 2009 年制定的健康資訊外洩通報規則(FTC's Health Breach Notification Rule)，包括經營線上平台供人儲存不同來源個人健康紀錄之平台業者(Vendor of personal

health records)、透過線上平台提供體重、睡眠等健康管理產品或服務的相關業者(PHR-related entity)或是提供涉及個人健康資訊之第三方服務業者(Third-party service provider)等，必須向 FTC 通報健康資訊外洩情形，相關通報要求與期限則與 HIPAA/HITECH Act 的規定一致[12]。

(四) 違反 HIPAA/HITECH Act 之相關罰則

為嚇阻資訊安全危害事件的發生，HITECH Act 修訂提高相關罰則，當發生違反相關規定的事件時，若未能於 30 天內修正相關危害情形，最高將面臨 5 萬美元之罰鍰，若違反事件重複發生則單一年度最高可開罰達 150 萬美元。若涉及詐欺或為取得商業或個人利益而販售、傳輸或使用個人受保護健康資料等犯罪行為，還可能面臨最多達 25 萬美元的罰款和 10 年之刑期。

最後，於 HITECH Act 中亦列舉下列三種情況，可不列入違反 HIPAA 隱私/資安規則之事件。

1. 機構內人員非有意的取得：當受管轄機構或其業務夥伴之工作人員於執行其經授權的業務時，無意中取得同一機構內其他人員傳輸之個人受保護健康資訊，且該名人員未再對外洩漏或使用該筆資料。

2. 同機構內非故意之揭露：經授權使用個人受保護資料之人員，無意中向同一機構內未經授權的人員揭露相關資料，且該受保護資訊未被使用或再洩露予其他人員。

3. 可信賴的揭露對象：當發生向未經授權的人員或機構揭露未加密的受保護健康資料時，若該人員/機構具有良好的信譽，可相信其不會保留該筆資料時。

歐盟之個資保護與網路資安管理新制

一、幾經變革後之新法上路

歐盟於 1995 年率先發布的「個人資料保護指令(Data Protection Directive, 95/46/EC)」，是世界各國修訂個人資料保護相關法制的主要參考對象，例如我國於 1995 年完成立法之「電腦處理個人資料保護法」以及後續修正通過的「個人資料保護法」，有部分條文係參考歐盟指令之規範精神而修訂[13]。

隨著資通訊科技的日新月異，網際網路的應用已逐漸滲透至日常生活的各種層面，近年物聯網和大數據應用的興起，更令施行已逾 20 年之個人資料保護指令無法應對此巨幅變化。因此，歐盟執委會自 2012 年啟動修法工程，歷經歐盟執委會、歐洲議會等多方協商討論後，終於 2015 年末達成修訂共識，並於 2016 年 5 月 4 日正式公布歐盟新制訂的「一般資料保護法(General Data Protection Regulation, GDPR, Regulation (EC) 2016/679)」[14]。此次歐盟修法將個人資料保護規範由指令(Directive)提升至法規(Regulation)層級，可以直接適用於各會員國，不需再透過各國制訂國內法加以轉換，將有助於減少各會員國的法律制度差異問題，此外，除於各會員國內成立單一監管機構外，歐盟亦將成立獨立的「歐盟資料保護委員會(European Data Protection Board, EDPB)」藉以維持歐盟區域內之資料保護法規一致性。但考量各會員國內的公務機關或非公務機關都需要時間以因應個資保護制度上之大幅變動，故特別將該法生效日期延後至 2018 年的 5 月 25 日，屆時將正式取代原先的個人資料保護指令。

另一方面，歐盟於 2016 年 7 月 6 日也公布了新的「網路與資訊系統安全指令(Directive on Security of Network and Information System, NIS Directive, Directive (EC) 2016/1148)」[15]，旨在加強各會員國內的關鍵基礎營運商及數位服務提供者之網路與資訊系統共通安全要求，並增進各會員國間資訊交換與合作之機制，各會員國最晚必須於 2018 年 5 月 10 日前，將指令之內容適用至各國法規並公布之。

二、歐盟一般資料保護法之管理新制

(一) 擴大適用對象與資料範圍

歐盟新的 GDPR 規範的對象包括自然人、法人、公務機關、機構和其他組織，並分

成決定資料使用目的之資料控管者（Data Controller）以及依資料控管者命令進行資料處理的資料處理者（Data Processor）兩種身分；資料控管者或資料處理者在歐盟境內設立之分支機構所為之個人資料處理活動都必須受 GDPR 規範，不論其實際的資料處理過程是否發生於歐盟境內；非設立於歐盟境內之機構若對歐盟境內的居民提供商品或服務並涉及個人資料的收集或對其所為行為的監控，也必須遵循 GDPR 的規範。

另一方面，GDPR 也同步擴大資料保護的範圍，包含全部或一部分以自動化方式處理之個人資料，或其他非自動化方式處理而構成檔案系統之一部分或旨在構成檔案系統之一部分可進行系統檢索之個人資料，資料內容則涵蓋：

1. 個人身分和生物特徵資料：如電話號碼、地址、車牌、健康資料、指紋、臉部辨識、視網膜掃描、相片、影片、電子信箱、電郵內容、問卷表單...等；
2. 線上定位資料：如 Cookie、IP 位置、行動裝置 ID、社群網站活動紀錄...等。

同時，GDPR 也將當事人所為單純之個人或家庭活動，以及主管機關為達預防、偵查或追訴刑事犯罪或執行刑罰之目的所為之個人資料處理列為排除適用的項目，以減少民眾及公務機關合理使用的限制。

(二) 大幅增加當事人權利

歐盟 GDPR 除了擴大納入管理的個資範圍，也同時大幅度提高當事人的權利，包含可要求知悉資料控管者的身分以及資料使用的目的等，有關資料處理的任何資訊或聯繫方法，也應獲告知其可能的風險和應有的權利和行使的方法，以符合個人資料收集、利用、處理的「透明原則(principle of transparency)」。此外，GDPR 也賦予當事人向資料控管者請求存取使用其被收集處理之個人資料的權利(right of access)，資料控管者有義務於一個月內回應當事人的請求，必要時得延長二個月，並應免費提供當事人個人資料副本一份，如有更多份數之要求才能收取合理之費用；同時，當事人也有權要求將其個人資料移轉至其他資料控管者(right to data portability)。當個人資料不正確或不

完整時，當事人也有權利要求資料控管者進行更正或使其資料完整(right to rectification)。

另一方面，本次 GDPR 修法最大的亮點之一，就是賦予當事人「被遺忘權(right to be forgotten)」，若當事人因對於收集與處理其個人資料的目的，不再有需要或遭違法處理等因素，可拒絕或限制資料控管者處理其個人資料，甚至可撤回對個人資料處理之同意並要求刪除其個人資料，不再被納入自動化分析處理的範圍。有鑒於大數據分析及 AI 科技興起，GDPR 也特別允許當事人有權要求在基於資料分析進行決策的過程中增加人為參與、表達意見以及挑戰該決策之機會，而不受僅基於自動化分析處理(automated individual decision-making)所做成而對其產生法律效果或類似之重大影響之決策所拘束。

(三) 個人資料保護原則與合法要件

為達到對當事人權利之保護，CDPR 明確定出個人資料處理應遵循下列原則：

1. 合法性、公正性與透明性(lawfulness, fairness and transparency);
2. 目的限制(purpose limitation);
3. 資料最少收集(data minimization);
4. 正確性(accuracy);
5. 儲存限制(storage limitation);
6. 完整及保密原則(integrity and confidentiality);
7. 舉證責任(accountability)

資料控管者處理當事人個人資料時，必須符合 GDPR 的規範，且須明確告知當事人資料處理的目的、收集的資料範圍、處理後資料的接收者等訊息以獲得當事人同意，

實際進行資料處理時，僅能用於經當事人同意之目的，不能做為其他目的之延伸使用或處理，且收集的資料內容必須限於該處理目的所必要之最小範圍，並要確保資料的正確性、完整性與機密性；保存資料的期限也不得長於該處理目的所必要之期間。此外，資料管控者或資料處理者負有自我舉證的責任，必須證明自己確實遵守上述 GDPR 的要求，否則將面臨相關之罰則。但若是專為新聞、學術、藝術或文學表達目的所為之個人資料處理，則得排除在 GDPR 規定之外或豁免之。

其中，GDPR 所規定的合法要件包括：

1. 取得當事人明確之同意，過去所允許的默認同意設定將不再被視為合法；
2. 履行與當事人所簽訂契約或為簽訂契約所必須；
3. 遵守法律規定義務所必須；
4. 為保護當事人或他人之重大利益所必須；
5. 為符合公共利益執行職務或行使公權力
6. 於不違背當事人基本權益及自由下，追求正當利益之目的
7. 為符合公共利益、達成科學或歷史研究目的或統計目的所為個人資料處理，應受本規則所定適當保護措施之拘束

(四) 應採取之安全維護措施與認證機制

為確保個人資料的安全，這次 GDPR 修法已將「設計(by design)與預設(by default)資料保護原則」納為安全維護措施制定之重要精神。資料控管者或資料處理者必須採取科技化且有組織之措施，例如使個人資料假名化(Pseudonymisation)等加密技術，確保系統及服務持續之機密性(Confidentiality)、完整性(Integrity)、可取得性(Availability)及彈性(Resilience)；並須在事故發生後及時回復個人資料的可取得性(Availability)及可使用性(Access)，同時也需定期評估、測試、衡量及確保安全措施之有效性。此外，GDPR

也規定若資料控管者或資料處理者需要定期且系統性的大規模監控當事人，或需大規模處理包含基因資料、生物特徵識別資料、與健康相關等特殊資料時，資料控管者或資料處理者應指定具備專業資格之資料保護專員(Data Protection Officer)，並應於資料處理前實行個人資料保護影響評估(Data Protection Impact Assessment)。若評估結果發現若未採取降低風險之措施，該處理可能導致高風險時，資料控管者應於資料處理前事先諮詢監管機關。

另一方面，GDPR 中亦新設相關條文，將推動資料保護行為守則及認證機制之設立，並賦予行為守則制定機構或認證核發機構得對承諾遵守該行為守則或安全認證之機構進行強制性監測，對資料控管者或資料處理者所為之認證，最長期限應為三年。資料控管者和資料處理者得以取得該行為守則或資安認證，作為其遵循 GDPR 安全維護要求之證明文件。

(五) 發生個資侵害事件之通報要求與相關罰則

當發生個人資料洩漏或不當使用等侵害事件，可能導致當事人權利及自由之高度風險時，資料控管者應主動與當事人聯繫說明個人資料侵害情形，不得無故遲延，同時資料控管者應於 72 小時內向監管機關通報；但若危害情形不會造成當事人權力及自由侵害之風險，則不在此限。資料控管者也應記載任何個人資料侵害情形，包括與個人資料侵害相關之事實、其影響及已採取之救濟措施。前述之記載必要時得由監管機關查驗是否符合規範要求。

當違反有關資料控管者及資料處理者之義務，最高得處以 1000 萬歐元之行政罰鍰；如為企業，則可處以前一會計年度全球年營業額之 2%，以較高者為準；若涉及非法處理個人資料、違反個人資料國際傳輸規定、侵害當事人之權利等行為，則可能面臨加重處罰，最高可達 2000 萬歐元或前一會計年度全球營業額 4%。

三、網路與資訊系統安全指令

(一) 推動建立歐盟內部網路安全合作與資訊交流平台

歐盟除了前述備受關注的 GDPR 外，新的 NIS 指令也將於今年 5 月正式生效。該指令要求各會員國必須訂立網路與資訊系統安全之國家策略，並須設立至少一個國家級網路與資訊安全監管機構(Competent Authority)，並指定其中一個機構為新設立之歐盟網路安全合作小組單一聯繫窗口，同時也必須設立至少一個電腦安全事件因應小組(Computer Security Incident Response Teams, CSIRTs)，負責監測國家資安事件、提供預警、因應及分析資訊，並參與新設立之歐盟電腦安全事件因應小組網路(CSIRTs Network)，作為各會員國交換資安資訊之平台。

此外，NIS 指令也要求各會員國必須提高其境內包含能源、運輸、銀行、金融市場設施、健康照護、飲水供應與分配、數位基礎設施等關鍵基礎服務營運商(Operators of Essential Services, OES)以及線上交易平台、線上搜尋引擎、雲端服務平台等數位服務供應商(Digital Service Providers, DSP)之網路與資訊系統安全，並須於 2018 年提出境內列管之機構名單，後續將每兩年定期更新。

關鍵基礎服務營運商(OES)的認定原則，包含提供維持社會或經濟活動之重要服務、依賴網路或資訊系統供應之服務、或是發生危害時會造成嚴重破壞性影響之服務等。其中有關嚴重破壞性影響之評估依據如下：

1. 依賴該項服務之人數；
2. 其他機構對該項服務之依賴性；
3. 對經濟、社會活動或公共安全造成衝擊的程度與持續時間；
4. 該機構之市佔率；
5. 可能受到影響的地域範圍；
6. 該機構對維持該項服務的可取代性。

(二) 針對關鍵基礎服務營運商與數位服務供應商之安全維護要求

NIS 指令中也提出被列管的關鍵基礎服務營運商(OES)所擔負之安全維護責任，包含應採取合適且合理的技術與系統化方法進行網路與資訊安全之風險管控、應採取合適的方法預防或減輕危害對網路及資訊安全的衝擊以確保能維持服務、以及當危害發生且對維持服務造成重大影響時，須及時通知監管機關或 CSIRT。

數位服務供應商(DSP)面對資安風險時，應具備適當的網路及資訊安全防範能力，包含需具備系統和設施之安全措施、侵害事件發生時之處置能力、維持營運所需之管理能力、定期監控、稽核與監測能力、並能遵循國際相關標準，但以上要求不適用於 50 人以下或年營業額或資產總額小於 1000 萬歐元之小型企業。

結語

美國與歐盟各國皆為我國醫療器材之主要出口市場，隨著健康大數據與生理監測雲端服務的應用與普及，我國醫療器材業者亦逐漸脫離單純製造業者的角色，朝向成為整合服務的提供者，以創造更高的企業價值。2016 年底，美國國會通過的「21 世紀醫療法案 (21st Century Cures Act)」[16]，亦將數位醫療技術納入主要推動的方向之一，鼓勵電子醫療資訊與互操作性(Interoperability)醫療器材的發展與應用。2018 年 5 月歐盟之「一般資料保護法規」以及「網路與資訊系統安全指令」陸續生效後，新的個人資料與資安保護管理機制正式啟動，可預期將為世界各國的管理帶來新的思維與衝擊。美國與歐盟的健康資料管理法規，將是業者必須遵循的方向，後續實際執行與做法，值得國內各界進一步的關注與了解，或可成為我國主管機關研訂相關法規之參考。

參考文獻

1. 2017 MEDICA 全球醫療器材發展趨勢觀察, TrendForce Bio, 2018/04/02.
2. NHS cyber-attack: GPs and hospitals hit by ransomware, BBC News, May 13, 2017.

3. Global cyberattack strikes dozens of countries, cripples U.K. hospitals. cbsnews.com, May 13, 2017.

4. Facebook scandal 'hit 87 million users', BBC News, April 4, 2018.

5. Summary of the HIPAA Privacy Rule, United States Department of Health Human Services, Office for Civil Rights, July 26, 2013.

6. Summary of the HIPAA Security Rule, United States Department of Health Human Services, Office for Civil Rights, July 26, 2013.

7. American Recovery and Reinvestment Act, Title XIII, Division A, Health Information Technology, Title IV, Division B, Medicare and Medicaid Health Information Technology, USA, February 17, 2009.

8. 45 CFR Parts 160 and 164, United States Department of Health Human Services, Office for Civil Rights, January 25, 2013.

9. 16 CFR Parts 318, Federal Trade Commission, August 25, 2009.

10. Cybersecurity Act of 2015(Public Law 114-113), USA, December 18, 2015

11. 美國通過 CISA 網路安全法案，行政院國家資通安全會報技術服務中心, 2016/01/04.

12. Complying with the FTC’ s Health Breach Notification Rule, Federal Trade Commission, April 2010.

13. 法務部「歐盟及日本個人資料保護立法最新發展之分析報告」委託研究案成果報告, 東海大學, 2016/12/30.

14. 歐盟個人資料保護規則, 財團法人金融聯合徵信中心, 2017/07.

15. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, July 2016.

16. 21st Century Cures Act (Public Law 114-255), USA, December 13, 2016.