Deloitte.

勤業眾信

跨越疆界

探索數位醫療法規因應策略

目錄

前言

勤業眾信在2017年「勤業眾信生技醫療產業趨勢論壇」即以智慧醫療為題，探索跨界整合的營運模式。醫療器材及醫療照護是這波生技醫療的數位浪潮中率先受到影響的產業，許多國家在近兩年陸續頒布新法規，國際正面臨新舊醫療器材法規轉換的關鍵時期，而外銷金額正逐年成長的台灣醫療器材產業，該如何因應這潮流的轉變？面對國際醫療器材法規的重大變革，台灣業界似乎尚未有太多討論，尤其在數位醫療方面的新法規，也會影響到醫材供應鏈內的上游廠商，這對以代工為主的台灣醫材產業影響不小。

因此，勤業眾信生技醫療產業團隊集合專家之力，彙整美國、歐盟及中國數位醫療法規概覽，以及醫療器材數位化相關之規定，提供業界參考。最後，我們也從醫材產品生命週期出發，分別從策略規劃、品質管理、安全與隱私權保護以及其他風險等層面，提出台灣業者對國際相關法規變革的因應之道。期盼以此報告，協助台灣企業掌握國際數位醫療法規趨勢要點，作為產品開發及上市規劃之參考。

生技醫療產業負責人

生技醫療產業
風險諮詢服務執行副總經理

醫療器材產業的數位變革

人口結構高齡化、以及心血管、糖尿病等慢性病罹患人口成長等因素，預計全球醫療保健支出將以4.3%的年複合成長率，從2015年的7兆美元成長為2020年的8.7兆美元，主要成長來自於北美、西歐及亞太等主要經濟區域。勤業眾信發表的《亞洲之聲》（Voice of Asia）第三期報告則指出2027年亞洲老齡人口總數將由3.65億成長至5.2億，在高齡化趨勢使然下，也將成為65歲以上人口最多、成長速度最快的市場。為了緩解高齡化趨勢下勞動人口不足、醫療資訊分配不均、醫療費用成長等問題，數位科技的發展及行動裝置的普及，也為產業帶來了創新解決方案。

重視精準及整合，打造創新醫療照護模式

運用科技達到精準診斷與治療

近兩年來，相當熱門的「精準醫療」(Precision Medicine)議題，是目前全球醫界正在發展的方向。這個概念於2011年11月首度由美國國家研究委員會(United States National Research Council)提出。精準醫療利用更多的基因檢測，將病患分成不同族群，依基因變異，給與適合的藥物對症下藥。

美國已於2015年啟動了精準醫療計畫(Precision Medicine Initiative)，並預計投入2.15億美元，其短期目標為擴展癌症基因組學(Cancer Genomics)以發展更佳的預防和治療方法；而長期目標為建立一個知識庫，能全面涵蓋全美科學家網路，以及建立一個百萬人的生物資料庫以進行跨世代研究，藉以擴大對於健康和疾病的認識。在次世代基因定序技術大幅降價和AI晶片大量普及的今日，此計劃的研究成果將加速醫療診斷和治療，這也是促成生技醫療產業持續蓬勃發展的原因之一。

若藉由個人基因及生物資料大數據，先進的資通訊科技，運用人工智慧(Artificial Intelligence, AI)、穿戴式裝置搭配App以針對眾多的病例、檢驗數據、醫療影像等臨床巨量數據進行資料蒐集分析；其後判讀並分析眾多非結構化的生物資料，建立蒐集生理數據與臨床病徵的數據關聯性，以加強臨床診斷時效並提升病患照護的準確性，這對於尋求以患者為中心的個人化醫療服務有莫大幫助。

甚麼是精準醫療?

精準醫療係指除了透過傳統治療問診及常規檢測方式外，再搭配生物醫學檢測，並結合個人生物特徵(例如：性別、身高、體重、種族、個人病歷、家族病史、生活習慣等)，與人體基因資料庫進行比對，找尋最適合提供予病患的配藥及治療方法，以達最佳治療成效。例如，某患者求診於醫生，醫生最初因為病徵而開立三叉神經痛藥carbamazepine（Tegretol, 又稱癲通錠） 處方，卻未注意到病患對藥品過敏，導致服藥後第3天開始出現輕微發燒、喉嚨痛等症狀，最初以為是感冒初期，不以為意，而後竟出現口腔黏膜潰瘍、眼結膜紅腫、皮膚出現紅色斑塊且中央呈灰色變化等症狀；再度求診後才發現是因為服用該藥物，引發史蒂芬強生症候群。此症在台灣致死率高達30%，幸好最終及早救治，未造成遺憾。

從上述案例可知，過往醫師主要透過病患口述症狀及醫療經驗來推測病因，現今醫療則導入更多醫學資料的比對，包括圖像、生化數據或基因檢測數據，協助醫生掌握病因，除可快速正確處理病症，解決病患問題，減少醫療浪費以外，更能進行遠距醫療、解決偏遠地區醫生人力不足問題，並讓醫生有更多時間投入治療及臨床研究，加速醫療科技發展。

醫療價值轉為重視病患需求、提升醫療體驗

透過數位科技導入，醫療院所的思維也正經歷一場變革。長久以來，健康照護模式是以醫院體系為核心，且與病患關係是趨向主導的一方，病患對疾病相關的資訊僅能透過醫院了解及取得。從病患角度來看，由於數位平台普及，病患可透過上網廣泛接觸醫療診斷與治療案例，並快速找到相關資源。病患藉由學習「久病成良醫」，加上市場對健康照護價值驅動轉以病患為中心，醫院得提供更透明的資訊，輔以數位化平台強化醫生與病人的溝通管道，以建立良好的「顧客體驗」。Deloitte報告就曾指出，醫院的績效與病患體驗評比有高度關聯性，也就是說當醫院應從提供病患較佳的健康照護體驗為出發，其績效表現也更好。

此外，在實際醫療場景，如手寫醫囑潦草影響後續判讀、口頭醫囑傳遞失準、影像判讀誤差、診療人為作業疏失等因醫療人為失誤所引起的醫療糾紛案例層出不窮；加上醫院長期人力資源不足，且醫療科技日新月異，專業人員需要短時間學習大量的專業新知。資通訊科技的突破，以及人工智慧(AI)的發展，各界亦期待上述問題可有效解決，提升醫療效率。

預防重於治療，打造全方位的數位健康管理策略

隨著健康意識的抬頭，事前預防的保健醫療觀念也逐漸普及，多數民眾會於平時定期接受檢查，以保養並監控生理狀況。此外，隨著社會人口結構逐漸邁向高齡化，健康照護資源需求攀升，多數高齡患者傾向選擇居家照護。隨著數位科技進步與物聯網帶來的契機，結合醫療技術突破，將有機會改變以醫院為主的現行照護模式，使照護範圍從醫療院所延伸至居家環境。

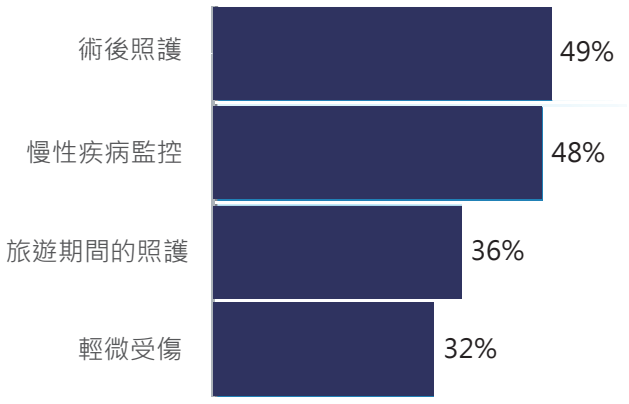
運用數位科技的感測裝置，將健康照護服務與物聯網應用結合，被照護者可於家中與工作環境等活動場所，接受遠距醫療(Telemedicine)、遠距病患監控(Remote Patient Monitoring, RPM) 等健康照護管理服務，節省往返醫院的時間與金錢成本，進而提高被照護者的配合意願，提高後續照護的效率。

健康醫療App蓬勃的發展，也強化民眾在健康管理數位化上的活動。根據美國食品藥物監督管理局(Food and Drug Administration，全文簡稱USFDA)的估計，2016年全球已有165,000個健康相關的Apps，在Apple or Android平台上發布，並依據2017年的估計，已經有1.7億的下載次數。在國內，健康照護相關App應用也陸續發展，促進在宅健康管理。

醫療體系與病患對數位化醫療照護服務的看法

根據Deloitte於2016年對3,751名美國成年人進行線上醫療照護服務的使用習慣與偏好研究調查，報告指出已有七成受訪民眾有意願接受數位化的醫療照護服務，其中接受度最高的類別為透過遠距醫療提供術後照護及慢性疾病的監控服務。

圖一、接受度最高的數位醫療服務，為透過遠距醫療提供術後照護與慢性疾病監控

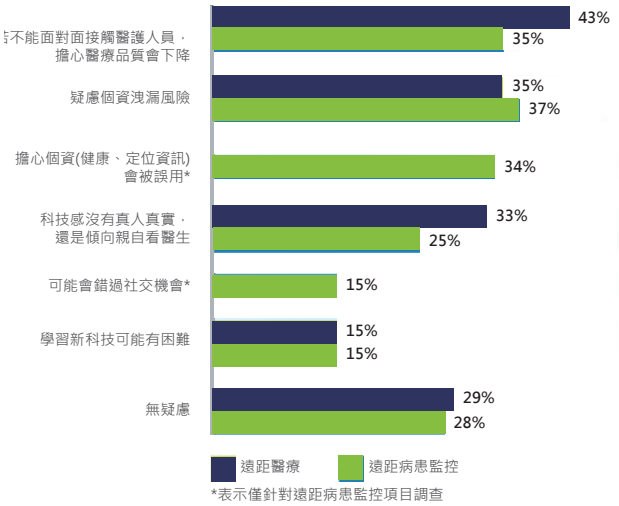


資料來源：Deloitte global, 2016 Survey of US Health Care Consumers

然而有些受訪者本身對此仍抱持懷疑態度，有三成受訪者提出對資訊安全疑慮，如：病患個資洩漏或誤用風險；有四成則是憂心醫療品質會因科技取代與醫護人員在醫院面對面接觸而下降。

有鑑於目前有38%的受訪者表示已有意願接受數位化照護服務，但僅有7%的照護者已開始使用，尤其在遠距病患監控(RPM)服務，可見未來仍有一段漫長的路要走。

圖二、採用數位科醫療服務的主要疑慮



資料來源：Deloitte global, 2016 Survey of US Health Care Consumers

跨產業整合，進而提高醫療品質

在這波數位科技浪潮推動下，除了醫療技術的創新突破，可讓醫療團隊有更多有效的資訊可供決策輔助，也健康照護模式出現轉變，讓照護範圍不再侷限於醫療院所，而是以病患生活為中心的場域。各國政府紛紛重視數位化對醫療照護產業帶來的影響，盼能達到「精準治療」以及「整合照護」的目的，進一步節省成本，優化人力等資源配置，並減緩醫療費用的增加。

其中，醫療器材產業更是生醫產業邁向數位化的先鋒。數位化對於醫材業者的挑戰會是：如何打造數位化的健康照護醫材，提供病患個性化與客製化的健康照護體驗，並能協助醫療團隊提高診斷與治療效益，以及協助醫院優化醫療人力資源配置、提供病患更高品質與有效的健康醫療服務。

醫療器材生態圈的轉型

因應人工智慧、穿戴式裝置與互聯網的發展，醫療器材與數位科技的結合成為各家醫療器材大廠切入的熱門趨勢。不僅醫療器材公司投入開發產品使用之軟體系統，許多高科技業者亦相繼投入醫療電子及智慧健康領域涵蓋範圍，不僅開發出如飲食紀錄、減重助手、舒眠工具、健康日誌等具監測及保健功能電腦及手機應用程式，亦跨入建置醫療照護單位的智慧醫療系統，如智慧病房、電子病歷與醫療影像管理等等。數位科技的發展也促使醫療照護服務提供者、醫療器材、製藥公司及高科技業者走向跨界整合，傳統醫療器材生態圈產生了重大質變。

數位科技所帶來的醫材新生態圈

傳統醫療器材生態圈是以醫療器材設備業者、驗證機構、主管機關、保險與支付者、消費者或病患，以及醫療照護服務提供者所組成，在嚴謹的法規監管機制下，進入者相對有限，且與其他產業的相關性較小。然而在互聯網及數位科技的發展下，各項個人保健用之軟體開發公司如雨後春筍般出現，醫材公司及製藥公司也開始嘗試將醫材或醫藥產品連結數位科技及行動裝置，藉以強化慢性病，如糖尿病或心血管疾病患者的個人健康管理。

因應這樣的趨勢，高科技業者也紛紛跨入醫療器材產業。尤其歐美國家對醫療器材的管理逐漸重視資料的

整合及可溯性，數位科技亦加速了醫療器材管理機制的改革。數位科技不僅使醫療器材業者面臨跨業合作的強勁壓力，與其他利害關係人的資訊交流也更加重要且密切，因此醫療器材公司在面對新生態圈的成形 (如圖三)，也需確保自身的數位化能力能跟上這波潮流。

圖三、數位醫療器材生態圈

資料來源：勤業眾信生技醫療產業團隊整理

以下簡述數位科技影響下的醫療器材新生態圈的主要角色：

- 醫療器材或製藥公司:醫療器材及藥品的開發及銷售公司，將產品結合數位科技，強化病患之個人健康管理。
- 保險與支付者: 可分為公家或私人保險業者，希望透過醫療健康數據分析，降低病患的醫療成本，並優化保險產品組合。
- 醫院與照護服務提供者:涵蓋公私立機構，透過數位科技監控並蒐集病患生理及醫療數據，藉由分析以提高醫療效率，降低成本。
- 消費者/病患團體: 藉由數位科技將生理資訊傳給服務提供者，達到監控及管理效果，提高醫療效率。
- 主管機關與驗證單位:主導或參與醫療器材管理機制，結合數位科技希望提高產品管理效率，並推動醫材產品的資料整合及可追溯制度，降低醫療器材不良反應的發生風險。
- 資訊分析服務: 涵蓋公私立機構，如CRO及學研單位，透過臨床及研究資訊的分享、蒐集與分析，建立資料庫，加速產品開發及更好的判讀結果。
- 軟體及系統供應者:提供合適的數位整合方案，加速醫療資訊蒐集及分析，以供個人或機構的專業人員判讀。
- 無線網路及晶片提供者:提供安全便利的雲端平台來供軟體或系統存取巨量醫療資料，使各個利害關係者在一定授權下分享及使用。

醫材數位化所面臨的風險

數位科技不僅促使醫療器材生態圈的轉型，網路安全與軟體設計漏洞也帶來新的衍生風險。近年陸續發生醫療器材因數位風險所引發的召回事件，主管機關紛紛重視醫療器材數位化之後所帶來的風險管理議題。

軟體確效風險

依據美國食物藥物管理署(US FDA)公布2016年所召回2000萬個單位醫療器材中，經分析召回原因主要可分為三大類，其中39.7%為產品品管問題，26%為軟體設計問題，22.6%為滅菌問題，隨著醫療器材軟體的高度應用，軟體設計問題在醫療器材召回比重逐年升

高。2016年美國前五大召回事件中，就有以下項目與軟體設計有關：

•因芮修第二代凝血酶原時間 / 國際標準比值專業型監控系統

為第一等級的召回事件，在美國召回的數量總共達125,576 個單位，召回原因主要為該系統可能產出偏低的數值，若產生較低的數值，則患者可能發生嚴重甚至致命性出血。

•Dexcom G4 PLATINUM Receiver

其主要功能為檢測糖尿病患者的血糖趨勢和葡萄糖模式，在美召回的數量為228,186個單位，主要召回原因為當檢測到超出正常範圍的血糖值時，接受器內的警報系統可能不會啟動，若依靠此產品通報血糖高低可能產生不良後果。

資訊安全風險

隨著醫療器材愈來愈高的比重會透過網路與醫院或其他醫療器材與智慧型手機相連結，醫療器材所面臨的網路安全風險也日益升高，甚至有些可能影響到醫療器材的正常運作。

2017年由於資安漏洞，美國FDA大舉召回約50萬個心律調節器主要原因在於這些心律調節器很有可能發生被駭客攻擊的風險，駭客利用心律調節器的設計漏洞，重新編程後，可停止心律調節器電池之運作或者修改患者的心臟跳動方案。雖然本次召回前還沒有心律調節被駭的消息傳出，但即使本次召回更新後，製造商還是需要持續針對這些可能的威脅與漏洞進行監控，以便確保心律調節器的正常運作及患者健康。

隱私保護風險

近期美國FDA核准了首例含有攝取追蹤系統(drug with a digital ingestion tracking system)數位藥丸，用以了解服藥狀態。用藥者可以運用App進行檢視，也可以選擇性將資訊分享給照護者或醫生。此舉雖被視為醫療保健與科技整合的重大突破，卻也有認為該藥品將對隱私造成疑慮。

美國前人類與健康服務部門 (Department of Human and Health Services) 的隱私長就建議應該詢問「資料怎麼流動的？訊號會發送至哪裡？如果資料會存放到某個人的伺服器，那伺服器在哪裡？商業模式上的安排為何？」從此亦可觀察各界對於數位醫療、醫材與醫藥間的疑慮。

國際數位醫療法規與國際標準變革

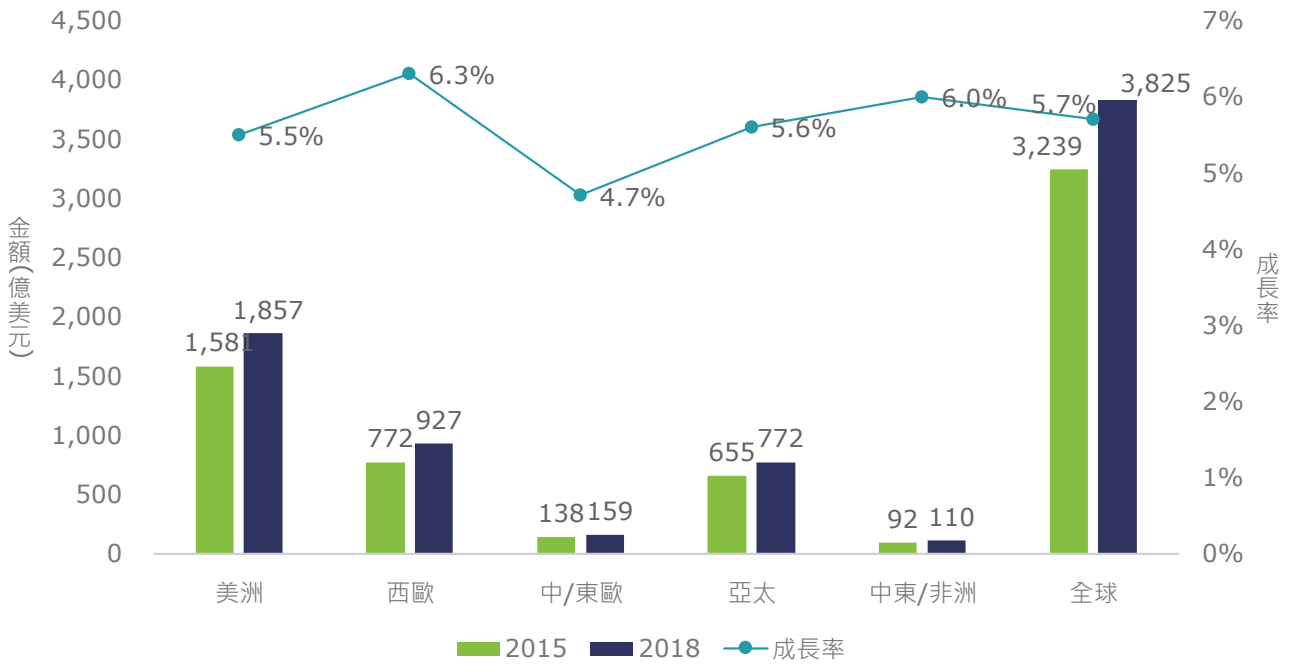
基於提升醫療在預防、回應上之效率，各國多開始推動醫療、醫材數位化，促使傳統醫材業者嘗試加入偵測設備、軟體、網路以及數據等功能，進入數位醫療領域，提升價值；資通訊業者也從數位手環、手錶等穿戴式設備，試圖進入健康照護與醫療領域，提供更個人化之預防、照護服務。台灣具備資通訊產業優勢以及育成機制，配合政府推動5+2創新產業政策，建構台灣成為亞太創新高值醫材產業重鎮，目標於2020年達到2,000億元產值。惟因醫療牽涉人身安全，因此對於數位醫療本身可能產生的風險，各國亦陸續開始制定法規加以管理。

根據圖四全球醫療器材市場規模分布的統計，全球市場中仍以美洲、西歐以及亞太區為重要的市場。而亞太區中，又以中國市場的成長潛力可期，故以下主要探討美國、歐盟及中國之數位醫療相關法規概況。

美國數位醫材法規環境概觀

美國自歐巴馬時代發布《21世紀法案》(21st Century Cures Act)後，奠定了數位醫療法規發展的基礎。在此基礎下，美國醫療器材主管機關，USFDA為透過正確的政策，促進安全以及有效的創新活動，因此於2017年7

圖四、2015及2018年全球醫療器材市場規模分布及成長率預測



資料來源:BMI, 2016年; 工研院IEK, 2016年5月

月，提出了《數位醫療創新行動方案》(Digital Health Innovation Action Plan)，專注於鼓勵藥品與數位健康科技的創新。FDA期望透過這個計畫，達到以下目的：

- 讓用戶能對於健康、日常生活習慣監控與慢性疾病管理能做出更好的決策、或者能夠與醫療專家連結互動。目標是應用用戶導向的軟體與其他技術，幫助人們活得更健康。
- 透過決策支援軟體以及相關技術，讓臨床實務、決策、診斷與發展處方、管理、儲存、分享健康紀錄，以及行程、工作流程安排能夠更好且更有效率。
- 協助處理如流感類的公共衛生危機。

USFDA對於數位醫療的內涵定義為「行動醫療、健康資訊科技、穿戴式設備、遠端健康與遠端醫藥、以及個人化醫療」。為了確保數位醫療所帶來的效益與風險間能有所平衡，USFDA已針對以下領域開始進行研討，並逐步建立監管架構：

- 無線醫療器材(Wireless Medical device)
- 行動醫療用apps (Mobile Medical Apps)
- 醫療資訊系統 (Health IT)
- 遠距醫療 (Telemedicine)
- 醫療器材資料系統 (Medical Device Data Systems)
- 醫療器材的互通性(Medical device Interoperability)
- 醫用軟體(Software as a Medical. Device, SaMD)
- 一般健康 (General Wellness)
- 網路安全 (Cybersecurity)

為了能夠有效地推動數位健康技術，美國於推動智慧醫療的策略上，採取有效的、基於風險的監管方式，並較為寬鬆的政策。也因此，USFDA亦推動「認證前軟體試驗」(Pre-Cert for Software Pilot)計畫，由Apple、Fitbit等九家大廠參與，以加速創新，並同步採用指引，期盼逐步建立產業標準。從此態勢，可觀察USFDA對於智慧醫療法規的態度，以促進創新為優先，並在可受控的環境下，逐步開展適合該類產品的風險規範。

歐盟數位醫材法規環境概觀

歐洲則由歐盟委員會（European Commission）的衛生暨食品安全總署（DG Health and Food Safety, DG SANTE）推動整合性計畫，於2012年提出《數位醫療行動計劃2012-2020》(eHealth Action Plan 2012-2020-Innovation healthcare for the 21st century)作為基礎。在這份計畫中，歐洲提出的數位醫療（eHealth）內涵為：「基於健康照護體系與新技術下，於健康相關的產品、服務與流程中運用資通訊技術，以提升公民的健康、健康照護產業的效率與生產力，以及健康帶來的經濟與社會價值。」在這個體系下，數位健康包含了病人、健康照護服務提供者、機構對機構間的資料傳輸，或病患與健康照護專家間點對點的互動。

此外，在計畫書中也提到了歐盟推動eHealth可能遭受的障礙：

- 病人、公民與健康照護專家間缺乏對於eHealth的認知與信心；
- 缺乏eHealth解決方案的互通性(interoperability)；
- eHealth工具與服務帶來的效率證據有限；
- 對於健康與福利的行動應用軟體需要近一步釐清相關管理法規，目前此類行動應用上對所蒐集資料之有效運用還不夠透明；
- 不適當或分割的法律架構，包含對eHealth設備軟體

報銷的方法還未有明確規定；

- 設立eHealth系統的初始成本高;
- 存取資通訊服務上有區域性的不同，較貧困區域的存取服務會有限制。

該計畫中提出將透過數位醫療網絡(eHealth Network)的方式來加以因應，措施包含：

- 跨境醫療照護指令(Cross-Border Healthcare Directive：作為eHealth Network運作之基礎，給予病患於其他歐盟會員國接受治療之權利，強化電子健康系統以及照護上的互通性，並確保安全與品質健康。
- 推動歐盟技術以及語意的標準，以促進互通性測試以及認證
- 檢視成員國對於電子病歷的法令，以促進互通性；
- 檢視公民與病人的資料保護規定，討論在存取或再利用健康資料進行研究時，其資料擁有權、資料控制等，並且將雲端運作架構納入考慮。
- 定義「行動健康」和「健康與福利」應用的相關法律問題

在歐盟層級下牽涉e-health的法規則包含以下內容：

- 《一般資料保護法規》 (General Data Protection Regulation,GDPR)：規範歐盟地區隱私保護之要求
- 《電子商務指令》(The E-commerce Directive, Directive 2000/31/EC)：規範遠距醫療相關做法
- 《醫療器材法規》(Medical Devices Regulation, MDR; Regulation (EU) 2017/745) 及《體外診斷醫材法規》(In Vitro Diagnostic Medical Devices Regulation, IVDR; Regulation (EU) 2017/746)：2016年公布，2017年5月正式生效，改善原有醫材法規。是現行醫療器材與體外診斷器材之主要法規
- 《遠距契約消費者保護指令》(Directive on Distance Contracting, Directive 97/7/EC)：遠端合約相關規範，用以支援遠程醫療或者是行動醫療的責任界定
- 《電子簽章指令》(Directive on Electronic Signatures)：電子簽章相關規範
- 《競爭法》(Competition law)：反不當競爭的相關規範

前述法規中，近期則以隱私保護以及可穿戴式設備相關規範的變更較為顯著。

中國數位醫材法規環境概觀

現行中國對於智能醫療之定義為：「通過打造健康檔案區域醫療資訊平台，利用最先進的物聯網技術，實現患者與醫務人員、醫療機構、醫療設備之間的互動，逐步達到資訊化。在不久的將來醫療行業將融入更多人工智慧、傳感技術等高科技，使醫療服務走向真正意義的智慧化，推動醫療事業的繁榮發展」。

中國現行推動醫療改革的基礎，係以「健康中國2030規劃綱要」的內容為主。其中牽涉智能醫療則描述於第七篇中，包含如下：

- 第二十三章「推動健康科技創新」：

加強慢病防控、精準醫學、智慧醫療等關鍵技術突破等目標；另也預備建成統一權責、互聯互通的人口健康資訊平台、建立遠端醫療應用體系。到2030年，實現國家省市縣四級人口健康資訊平台互通共用、規範應用，人人擁有規範化的電子健康檔案和功能完備的健康卡，遠端醫療覆蓋省市縣鄉四級醫療衛生機構，全面實現人口健康資訊規範管理和使用，滿足個性化服務和精準化醫療的需求。

- 第二十四章「建設健康資訊化服務體系」：

加強健康醫療大數據應用體系建設，並加強健康醫療大數據相關法規和標準體系建設，強化國家、區域人口健康資訊工程技術能力，制定分級分類分域的資料應用政策規範，推進網路可信體系建設，注重內容安全、資料安全和技術安全，加強健康醫療資料安全保障和患者隱私保護。加強互聯網健康服務監管。

近期中國牽涉創新醫療器材與智慧醫療的法規、意見或指引，包含：

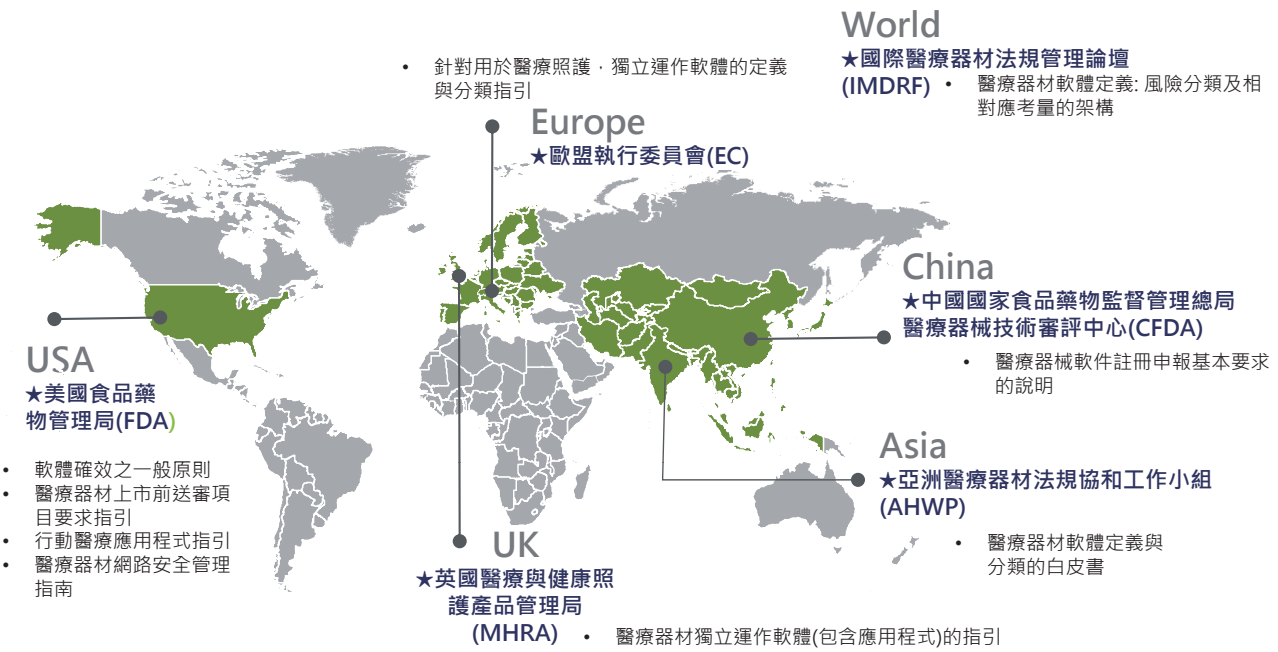
- 創新醫療器材特別審批程序：針對創新醫療器材的審批規範
- 於深化審評審批制度改革鼓勵藥品醫療器材創新的意見：鼓勵藥品醫療器材的創新改善
- 醫療器材網路安全註冊技術審查指導原則：網路安全相關法規，針對需要聯網之設備，明確定義其資訊安全相關要求
- 人工智慧輔助診斷技術管理規範：規範人工智慧的應用並定義相關的應用質量控制指標。
- 互聯網醫療保健訊息服務管理辦法：規範互聯網上提供醫療保健訊息的執行要求
- 關於推進醫療機構遠程醫療服務的意見：推動醫療機構於互聯網上提供遠程醫療的說明

除前述規範外，中國目前的法治環境採先放後管，目前已有對於互聯網上的診治行為，發出「互聯網診療管理辦法(試行)徵求意見稿」，強調遠距醫療須由醫療機構提供，並定義資料保護、人員管理等要求。後續仍須持續關注法規上的變化。

法規變革重點觀察—軟體確效

因應醫療器材持續發展，各國均發布醫療器材相關標準規範，且因醫療器材軟體疏失可能危害使用者生命安全，故針對醫療器材軟體管理成為近期趨勢，如圖五所示，全球各國已逐漸重視醫療器材軟體的上市管理。因此，如何在醫療器材的生命週期各階段中，確保軟體管理的妥適性、可靠性、完整性與安全性，即是產業發展思維中不可或缺的一環。以下則介紹美國、歐盟及中國之相關規定。

圖五、全球醫療器材近年制定軟體上市前審查相關之指引



資料來源：勤業眾信生技醫療產業團隊整理

各國醫療器材軟體確效法規概覽

- **美國**

美國USFDA於2017年8月發布醫療創新方案 (Medical Innovation Access Plan)，其中一項議題便是致力於建立規範創新型醫療產品安全性和有效性的標準，讓創新醫材能在更友善的環境中發展，如：FDA 提出醫療設備開發工具 (medical device development tool, MDDT) 認證，為醫材相關開發設備提供一個更客觀的平台，通過認證的工具能更有效協助業者發展產品，例如減少實驗動物的試驗、減少研發時程或樣本量等。

- **歐盟**

以歐盟而言，醫療器材法規(MDR)及體外診斷器材法規(IVDR)於2017 年 5 月正式生效，新法規大幅提升有關醫材認證的規範與限制，例如關於醫材分級便增加至超過 20 條規範，增加醫材產品的可追溯性、臨床試驗規範嚴謹度、臨床證據的掌握度與增加上市後的產品安全性與效能監督。

- **中國**

中國2015年發布《醫療器械軟體註冊技術審查指導原則》，發現中國對醫療器材軟體要求更加明確，將軟體生命週期管理概念納入法規，更強調軟體發布與更新的管理方式，依據中國醫療器材軟體定義的軟體安全性級別，進行不同程度的風險控制手段。2017年4月，中國發布《醫療器械標準管理辦法》，其中亦強調技術要求。

國際醫療器材軟體確效相關標準現況

- **醫材品質管理系統標準 ISO 134585**

2016年發布的ISO 13485，新增有關軟體確效的條文要求，從過往的醫療器材本身軟體品質控管，延伸到對醫療器材生產、監督與測量過程中的軟體均屬其要求範圍內，另主要管理重點如下：

1.生產與服務提供過程中的確認

當醫材器材軟體生產與服務提供時，須建立一套機制與程序進行後續的驗證，其驗證程序從產品生命週期觀點出發，須包含評審與批准的準則、驗證方式與過程變更與相關紀錄的要求等不同階段的要求。

2.監視與測量設備的控制

在醫材器材軟體生產與服務提供的過程中，為確保產品服務品質一致性，需要確認監視與測量過程的作業方式，主要目的為透過一致的監視與測量標準，確保產品的校準與驗證方式可趨於一致，從標準的訂定方式、到校準的過程以及失效的處理方式，都可強化產品服務，讓產品服務品質可以維持在一定標準內，進而達到國際標準與客戶要求。

3.紀錄的留存與控制

上述各項確認過程，都應該具備完整的紀錄，主要重點如下：

⑴確認管理活動有效進行之證據

⑵具備文件制定的程序，以規定紀錄的標識，儲存，安全和完整性，檢索，保存期限和處置所需的控制

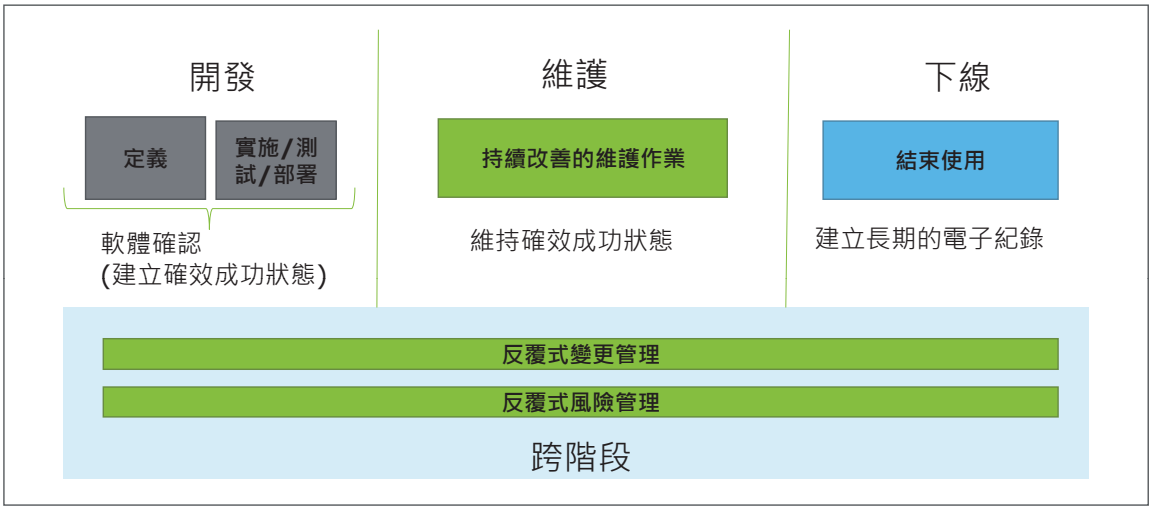
⑶留存清晰，易於識別和檢索的紀錄，包含紀錄變更的識別

⑷按法規要求，應實施健康機密資訊保護的作業方法

- **醫療器材軟體確校標準 ISO-80002-2**

今年(2017)　ISO亦發布了醫療器材軟體之軟體確效標準 (ISO-80002-2)。此標準之重點在於使用以風險為本的批判性思維來確定哪些活動應該執行，以充分確認特定軟體安全性和製造商合規性，其中「批判性思維」意指透過分析和評估軟體的各個方面以及相應的環境，確保醫療器材軟體之有效性。

圖六、醫療器材軟體生命週期管理



資料來源：勤業眾信生技醫療產業團隊整理

從醫療器材軟體的生命週期(如圖六)來看，醫材軟體管理標準IEC 62304強調對醫療設備軟體發展與維護的管理，其中包含從顧客需求管理、系統發展管理、軟體風險管理、軟體問題的管理、軟體維護需求的管理與後續作業都在其範疇中，故於戰略思考上應統合上述兩者，可分為下列管理重點：

1.開發階段

應定義何謂軟體確效成功之狀態，從流程需求定義，到軟體開發的實施、測試與部署，如何確認軟體的開發符合需求，希望藉由此階段的作業，讓開發人員明確理解哪些檢測項目在範圍內，而何者又在範圍外，能集中資源醫療器材軟體開發。

另須確保流程故障風險分析能於此階段完成，從危害風險，監管風險和環境風險角度出發，進行對應之確效活動規劃，並能夠在開發階段進行驗證，以確保流程故障風險能被妥適的管理，確實留存確效之紀錄，以達到有效監管。

2.維護階段

應維持軟體確效的成功狀態，在醫療器材軟體進入維護的週期時，過程中的變更活動均需進行適當之管控，其中包含但不限於錯誤的修正更新、性能或可維護性的提升、因應軟體操作環境對應之修正，於各項狀況中，應統合考量對預期用途和故障風險的影響，並規劃適當的機制來維持軟體確效。

維護階段可能發生緊急變更，醫療器材軟體供應商可能沒有足夠的時間進行完整的軟體確效程序，而組織應考量變更後之因應方式與對應之處理計畫，以確保醫療器材軟體能確實發揮功能。

3.下線階段

應確保系統下線後之電磁資料能有效保存，於醫療器材軟體後續須進行資料調閱或究責時，能提供可信且完整之歷程紀錄。

4.跨階段活動

於各個階段執行的過程中，均須考量反覆式的變更管理與風險管理活動，主要目的是希望在各個階段的作業活動中，均能妥適考量醫療器材軟體之商業目標與法規要求，確保各項活動的執行符合最初的需求。

法規異動對企業的影響

面對法規與各項國際標準的異動，對醫療器材軟體供應鏈中的企業而言，最重大的影響主要如下：

1.符合市場要求

對於公司既有或新創之產品，需確認目標市場之要求，以因應醫療相關法規變動，確立企業未來發展策略與規劃，避免發展受阻。

2.確認醫療器材的定義與分級

若法規異動涉及醫療器材的定義，公司應全面檢視產品線，確認產品分類，以利公司內部作業機制之調整。

3.建立軟體確效機制

依照前述要求，應考量目標市場，建立相應的軟體確效執行方式，並須留意除醫療器材本身的軟體外，用以支援、驗證或生產之軟體也在確效範圍，以優化利用公司資源配置，進行有效的產品布局。

法規變革重點觀察—資訊安全

隨著物聯網及數位科技的影響，智慧醫療已是重要發展趨勢。現今不少醫療設備皆具備感應、數據蒐集及通訊功能，結合感測和IT技術將醫療器材相互連接，透過巨量資料的蒐集與分析，電子數據交換或遠端控制，對於醫療模式有大幅度的變更，如遠距醫療、行動醫療，穿戴式裝置等推動數位醫療的發展。其中資訊安全是智慧醫療推動關鍵，數位醫療器材的運行必須有完善的法規可遵循，以下針對資安層面的醫材法規進行介紹。

各國資訊安全相關法規概覽

- **美國**

USFDA於2016年12月28日發布《醫療裝置上市後網路安全管理指南》(Postmarket Management of Cybersecurity in Medical Devices)。該法規主要在保障醫療裝置從開發階段到整個產品生命週期的網路安全，內容包含USFDA對於醫療裝置製造商的管理建議，例如製造商應監控、辨識與修補網路安全漏洞來管理已上市之醫療裝置。

而指南中也提出一種風險評估架構，供醫療裝置製造商在發現網路安全漏洞時，評估需向FDA通報之裝置修補變更。需要通報的情形為可能危及病患健康、或是造成死亡的嚴重漏洞，而定期的網路安全更新或漏洞修補不需特別通報。

該指南中明訂，醫療裝置製造商應:

- 監控與偵測裝置上的網路安全漏洞
- 了解、評估及偵測安全漏洞對病患帶來之風險
- 建立和資安研究人員的合作程序來接收潛在的漏洞資訊
- 訂定因應措施以盡早解決網路安全問題

最佳的做法就是在醫材的產品生命週期管理中納入網路安全考量，從裝置的開發設計階段就考量相關的網路安全，並且持續監控上市後產品的網路安全問題，修補安全漏洞。此指南即是最佳實務的指引，但因其不具法律強制性，目前仍需醫療裝置製造商自行執行相關管控跟規範遵循。

- **歐盟**

歐盟醫療器材法規(MDR)及體外診斷器材法規(IVDR)於2017 年 5 月正式生效，因應技術發展增加很多重要改變，對產品安全、性能評估、臨床評價和上市後的安全性監視更加嚴格，也強化技術審查、要求產品供應鏈的可追溯性等。另外，也增加如醫療軟體、網路安全的規範，並新增有關軟體及軟體醫材的說明，以提高醫療器材的安全性和使用效能，對於醫材的資訊安全有顯著的影響。此兩項法規要求的重點如下:

- 在歐盟的專家參與下，對高風險的醫材實施更嚴格的上市前控制。
- 加強指定標準和負責認證醫療器材的認證機構的監督程序。
- 管理涵蓋某些非醫療產品（例如：變色隱形眼鏡片），但具有與類似醫療器材相同的特性和風險特徵。
- 參考國際指引，引進體外診斷醫療器材的新風險分類系統。
- 通過建立全面的歐盟醫療器材數據庫來提高透明度。
- 有關使用有害物質訂定更嚴格的制度。
- 在歐盟範圍內要求導入「植入物卡」，對植入式醫療器材的患者提供相關資訊，如產品識別碼、重要警示事項、產品預期生命周期等。

- 加強臨床調查規則，包括在多個會員國進行的醫療器材臨床調查許可協議。
- 加強對製造商的要求，收集和分析有關其醫材實際使用的數據。
- 加強會員國在上市後監督領域的協調。
- 引入UDI（單一識別）系統，強化醫療器材可追溯性系統。
- 賦予經營者的角色和責任，以及授權代表履行新義務。

- **中國**

由於中國並沒有明確規範醫療器材的網路安全法規，最新的《網路安全法》涵蓋所有與網路安全相關的規定，因此在中國的醫療器材製造商也必須遵守《網路安全法》的相關規定，針對產品的安全認證、資訊的存取、以及個人資料的保護都應該有相應的管控措施。

中國政府則於2017年6月1日正式實施《網路安全法》，其中包含幾個重點:

- 個人資料保護

闡明對於個人資料蒐集、使用以及保護的要求

- 關鍵訊息基礎設施:

一旦遭到破壞、喪失或者數據洩漏可能嚴重危害國家安全、國計民生、公共利益的設施。此種設施的保護要求不斷在《網路安全法》中被提及。

- 網路營運者

網路的所有者、管理者和網路服務提供者的安全職責。

- 敏感資料保存

在境內蒐集或產生的個人資料，應保存在境內。

- 安全產品認證

網路關鍵設備和網路安全專用產品應在安全認證合格後才能銷售或提供。

- 法律責任

違反《網路安全法》的企業及組織機構，最高處罰金額可達100萬元人民幣。

國際醫療器材資訊安全相關標準現況

《健康醫療產業資訊安全標準》(ISO27799:2016)是ISO國際標準組織提供做為醫療產業保護其個人健康資訊的機密性、完整性、可用性的實務參考指南。ISO27799的內容是基於ISO/IEC 27002的控制措施，延伸至醫療產業營運環境所需要的資安管理做法。不僅可以滿足醫療資訊系統針對資療資訊的資安要求，也考量系統故障、網路阻斷服務攻擊、自然災害等相關議題，確保醫療資訊系統能夠安全與持續的運作。因此ISO27799也包含和ISO27002相同的十四項控制領域:

- 資訊安全政策
- 資訊安全之組織
- 人力資源安全
- 資產管理
- 存取控制
- 密碼學
- 實體與環境安全
- 運作安全
- 通訊安全
- 系統獲取開發及維護
- 共應者關係
- 資訊安全事故管理
- 營運持續管理之資訊安全層面
- 遵循性

ISO27799:2016是從政策和組織面開始強化管理系統，進而從人員、醫療資訊有關資產、以及存取的控管進行更全面的醫療資訊安全管理。而其中與醫療器材直接相關的控制措施如8.1.1「資產清冊」，提到必須識

別醫療器材的負責人，建立器材可被接受的使用方式與規則，並且考量在特定的環境中使用醫療設備，應避免受到不必要的電磁干擾而造成的威脅。而控制措施8.3.2「媒體之汰除」也提及在處理包含資訊的醫療設備，應採取安全的做法清除相關的資訊，以確保醫療設備的資訊安全。

法規異動對企業的影響

由於雲端與物聯網的蓬勃發展，各種產業也開始對於網路和資訊越來越依賴。而健檢中心、醫院、醫療器材製造商等醫療與健康資訊產業更應注意與人身安全有關係的資訊安全風險。

近期國內外已有多起針對醫院的網路攻擊事件，且數量持續增加。其中造成資料外洩的數量高達千萬筆，而受到惡意程式綁架的醫療裝置也多不勝數，例如核磁共振儀器、診斷使用的斷層掃描，都有被惡意程式攻擊的風險。因此，對於已逐漸高度資訊化的醫療產業，醫療器材的資訊安全相關控管是十分重要的議題，上述美國、歐盟、中國的法規對於當地醫療器材製造商以及使用的企業都有一定的影響。

例如美國的醫療裝置上市後網路安全管理指南(Postmarket Management of Cybersecurity in Medical Devices)，可以幫助製造商在產品生命週期中嵌入資訊安全的考量，也提供一個明確的做法讓業者可以遵循以確保醫療器材的資訊安全，雖無法律強制性，但若遵循該指南建立管理系統，可以幫助加強醫療設備之安全性，防止被攻擊者利用造成資訊安全、甚至是人身安全的威脅。

歐盟的醫療器材法規(MDR)及體外診斷器材法規(IVDR)，取代了舊有的法規，加強了體系面的管理、高風險設備的相關規定、以及提升產品對患者的透明度和可追溯性。對於想要布局歐盟市場的業者，這兩項法規的變動都會增加大量的工作量，然而藉由法規可以提升民眾對醫療器材的信心，並且加強審核過程本身的透明度和嚴格度。

中國的《網路安全法》則給企業帶來了許多不同的挑戰，例如企業原本只關注數據安全，現在須將範圍延伸到影響範圍更大的個人隱私保護；而《網路安全法》中提出了對關鍵訊息基礎設施的更高要求，對於使用醫療器材的醫療機構來說，也必須加強相關的管控；再者，中國政府要求敏感數據應該要儲存在中國本地，在數位醫療的跨國合作上增加了門檻；此外，《網路安全法》中明確規範了嚴格的處罰規定也使得企業必須立刻進行業務上的改進，否則可能有被停業的風險。

前述提及的各國法規以及國際標準ISO27799:2016，都是在近幾年內提出，對於企業來說，法規的發布會增加目前的工作量，並切需要對現有體系進行一系列改善，然而，隨著連網醫療設備的普及及增加，企業藉由遵循明確的法規及標準，進而將資訊安全管理嵌入醫療器材的產品生命週期，可以提升未來醫療器材市場上的產品品質管理，也能夠確保醫療器材的資訊安全，防範資安攻擊的威脅。

法規變革重點觀察—隱私保護

數位醫療的發展，讓患者與醫師、患者與世界各地的患者之間，有了新的數位化鏈結，而建立這鏈結關係的便是「數據」。由於牽涉個人基因及醫療數據，因此個人數據需要得到充分的保護，以符合相關國家和地區的隱私保護法律要求。各國醫療器材管理法規不盡相同，如何有效地保護患者隱私安全，不致於造成患者的隱私權遭到侵犯，也成為醫療器材發展過程中的主要挑戰。

因此，如何防止駭客入侵，導致病人數據被篡改，或臨床系統被破壞；或是避免因為系統的授權，而造成使用者濫用健康資訊檔案等，保障資訊安全與個人隱私將會成為醫療器材廠商發展的重要議題。多數國家在推動智慧醫療的發展時，除了同時強調病人隱私權、資訊安全保障，也應積極建立完善法規制度、資訊科技標準等，將相關資訊安全、法規、資訊標準的利害關係人納入智慧醫療推動的生態系統。醫療器材的專業廠商應遵循相關法令規定與國際標準，以下比較歐盟，美國和中國隱私法規的不同，提供借鏡參考。

各國隱私權保護相關法規概覽

- **美國**

如何在智慧醫療的發展下，將數據分析和患者隱私保護之間達到平衡，的確已成為一個亟待解決的議題，在美國，目前對病例數據的利用由《健康保險隱私及責任法案》(Health Insurance Portability and Accountability Act，簡稱HIPPA) 規範。這個法規是於1996年公告，任何機構(包含醫療院所或研發設計醫療器材之製造商)，只要需要製作、使用、受理、保存、傳輸「需受保護之健康資訊」(Protected Health Information, PHI)，就屬於「受管轄的機構」(covered entity)，必須遵循此法規之規範。

規範中同時對於所謂「可辨識的健康資訊」(Identifiable Health Information) 加以定義：任何資訊只要能夠足以評斷出特定個人的生理或心理狀態(不論是以口頭或其他紀錄形式)，就屬「可辨識的健康資訊」。法規中亦要求「必要的最小原則」(Minimum Necessary)，當必須將「需受保護之健康資訊」釋出、傳遞、提供、或給予外部單位使用時，除了是向本人揭露其自身之資訊、或醫療人員以治療為目的取得資訊、或依據個人授權而為之揭露或使用的這三種情況之外，各機構必須將PMI使用限縮到「所必要的最小程度」原則，進行資訊的提供與交換。各機構對於HIPAA的執行，均會受到民權辦公室(Office for Civil Rights)的監督。

HIPAA法案中也確立了一些強制條例，其中包括確立電子數據交換（EDI）、安全及所有醫療保健相關數據保密性的標準化機制。法案規定：病人的健康記錄、管理記錄和財務數據均採用標準化格式；每個醫療保健實體（包括個人、僱主、醫療計劃和醫療服務提供者）均採用唯一認證碼；運用安全機制確保識別每一個體的資訊數據具有保密性和完整性。另外，此法案亦規定儲存這類單位的實體不得在未經患者允許的情況下以銷售或研究為目的使用或出售患者的醫療記錄。一旦發生數據泄漏，該單位必須向政府報告，公司還必須與用戶達成隱私和安全使用協議。

- **歐盟**

歐盟對於病患隱私權的保護，可透過歐盟最新公告的《一般資料保護法規》 (GDPR) 來了解。即將於2018年5月正式實施的GDPR取代了過去的歐盟個人資料保護指令：Directive 95/46/EC，希望能更加落實自然人之個人資料處理及資料自由流動(於歐盟各會員國之間)之保護，確保此一基本權利與自由之保障。依據這份法規，醫療器材製造商對於資料庫所蒐集、處理、保存之基因資料、為了辨識特定個人之生物資料、健康資料，在規範中均被歸類為「敏感資訊」之特殊類別。

這類資訊，原則上禁止被他人處理及使用，除非以下幾種特殊情況：(1)資料提供者明確表示同意其資料為了一個或多個目的進行處理，並保有隨時撤回同意的權力。而取得其同意之機構，要能提具同意之證明。而有時科學研究在蒐集資料時，因可能無法立即有確定的研究目標，但若在科學研究的倫理性可以被確保的情況下，資料提供者可以同意將資料提供給某些的研究目的，或只同意其中某一部份。(2)資料處理對於重要的公共利益有其必要性，為了預防醫學、職業醫學、醫療診斷、治療或照護之提供、健康服務之目的，在成員國訂有相關法令規定之前提下，可以進行此類資訊之處理。有關資料處理之相關訊息，資料提供者必須被告知，且表達同意後，仍保有隨時撤回同意、要求資料修正、或資料刪除之權利。

- **中國**

中國國家食品藥品監管總局即將於2018年1月1日起施行《醫療器械網絡安全註冊技術審查指導原則》，醫療器材網路安全是指保持醫療器材相關數據的保密性、完整性和可得性。相關數據必須準確和完整，且未被篡改。醫療器材相關數據包括，標明生理、心理健康狀況，涉及患者隱私資訊的私人數據；以及用於監視、控制設備運作或用於設備維護保養等數據。

該原則要求申請人結合相關數據的類型、功能、用途、交換方式及要求，並結合醫療器材的產品特性考慮其網路安全問題，採用基於風險管理的方法來保證醫療器材的網路安全。此原則適用於具有網路連接功能以進行電子數據交換或遠端控制的醫療器材產品的註冊申報，重點著重於醫療器材產品生命週期過程中網路安全問題，包括醫療器材產品的設計開發、生產、分銷、部署和維護。

醫療器材對網路安全威脅應具備識別、防護能力，由於預期用途、使用環境的限制，其對網路安全威脅的探測、反應、恢復能力應當與其產品特性相適應。產品應在醫療器材全生命週期過程中確保醫療器材產品自身的網路安全，進一步保護患者個人隱私權利受到保障。

國際醫療器材隱私權保護相關標準現況

有關隱私保護的國際標準 ISO/IEC 29100:2011、個人資訊保護的英國標準 BS 10012:2017、雲環境下個人資訊保護的國際標準ISO/IEC 27018:2014 的要求，以及《個人資訊安全規範》，上述國際性標準規範所針對醫療機構制訂的醫療資訊安全管理標準，都強調在醫療機構進行資訊安全管理時，也需將個資保護概念融入，減少醫療資訊系統個資外洩之風險。

法規異動對企業的影響

隨著全球高齡化的趨勢，可望帶動包括智慧健康之醫材服務產業的發展，在2020年前全球相關產業有機會突破5千億美元的產值。數位醫療的發展，為醫療事業帶來新的動力和機遇。相關廠商在產品或服務的設計階段，即應做好「隱私衝擊評估」，並將「資料最小化原則」、「目的限制原則」、「資料安全維護原則」納入其中。

另外，針對數位醫療服務所面臨的獨特挑戰需有相應的防範措施，例如醫療器材的軟體開發或硬體設備本身存在的安全漏洞等原因，都有可能導致隱私洩漏，單純依靠廠商與醫院本身的管理自律不完全可靠，政府唯有建立嚴格的法律規範及完善監管體系，確實落實監管權責，進一步規範智慧醫療的技術指標、運行標準、服務評價、績效考核等，才可能較全面的保護患者的隱私不受侵犯。

台灣業者的因應策略

醫療器材業者面對數位化轉型的醫療應用趨勢，應在以患者為中心的觀念，評估與發展商業模式，並基於歐美主要國家醫療器材法規與相關國際標準變革的衝擊下，整體考量其影響，以採取應對措施，確保能滿足法規與國際標準的規範要求，方能成功數位轉型到下一階段，擴展企業的產品範疇與能量。

從生命週期管理建立因應對策

醫療器材從基礎研究、產品設計開發到臨床試驗、上市申請到量產與上市後管理，需經過一連串的階段與活動，面對前述的法規、國際標準與相關挑戰下，醫療器材業者應考量醫材行業的數位轉型策略，並由整體端對端生命週期的觀點，考量在產品設計開發階段中對於策略規劃、品質、安全以及其他相關風險議題如下圖J七。

圖七、醫材產品開發與設計生命週期各階段應考量之議題

資料來源：勤業眾信生技醫療團隊整理

策略規劃面之因應

隨著醫療產業邁入數位化，智慧醫療將是未來10年影響醫療保健產業成長的關鍵及驅動力，醫療器材業者應從策略面出發，思考規劃數位化轉型發展藍圖。

- **醫材行業數位轉型規劃**

數位轉型現已成為醫材業者在市場上競爭的利器，數位化轉型應考量各應用場景之設計與內部作業流程運作等因素，並制定數位轉型目標、制定行動計畫、生態圈合作、跨業協同合作、計畫監督管理、法規與風險管理議題掌握，進而讓醫材業者能有效轉型成為數位化組織。

- **使用者數位體驗及介面設計優化與App設計**

在以使用者為中心的智慧醫療發展下，醫療器材軟體的開發應運用服務設計思考(service design thinking)的方法與理念，幫助從使用者的角度整理各通路之定位，從數位介面、產品到實體通路挖掘出全通路中具有潛力和產品創新的機會點，打造符合使用者體驗的系統或App設計，進而提升使用者品牌忠誠度。此外亦須考量醫療器材軟體設計符合人因工程，以打造出滿足使用者需求之五感體驗(five senses)，並透過創新設計策略打造未來醫療器材軟體產品原型，透過可視化，減少初期開發之溝通成本，提高使用者體驗與滿意度。

品質管理面之因應

因應數位化轉型趨勢及醫療器材與物聯網結合的應用增加，醫療器材軟體開發更顯重要，如何配合產品上市時程規劃，開發高品質軟體且安全且合規的醫療產品，對於醫材業者是必須正視的議題。

- **醫療器材軟體開發生命週期管理**

醫療器材業者應該從軟體開發生命週期的角度來看，參考例如IEC 62304，導入醫療器材軟體生命週期管理，確保從軟體需求分析、架構分析、細部分析、單元測試、系統測試與軟體上線各階段所需活動執行及產出結果，此外另需針對醫療器材軟體上市後的維護作業進行管理，並且搭配風險評估，依據不同軟體安全等級導入對應的管理機制，以便在最適成本與資源投入下，確保軟體品質提供與風險的有效控管。

- **醫療器材軟體確效**

以往軟體確效主要著重在醫療器材軟體本身，但2016年發佈的新版ISO 13485，新增對於醫療器材品質管理體系中相關製造、監視與測量等相關軟體，也須進行軟體確效作業。醫療器材業者應依據不同風險等級之軟體採取對應能符合法規、國際標準及風險及成本考量的軟體確效做法，透過軟體需求、設計和測試各階段的驗證與確效程序，在早期及時發現可能產生的錯誤，確保醫療器材軟體確實測試其功能可達到預期與安全性，以避免器材故障時造成使用者的危害。

安全與隱私保護面

- **隱私設計（Privacy by Design）**

「隱私設計（Privacy by Design）」是歐盟近來年起所積極推動在服務與產品規劃設計時即融入隱私保護機制的概念，在2016年歐盟所通過的一般資料保護法規(GDPR) 亦此概念加入數據保護監管要求，透過隱私保護技術融入個資管理生命週期管理，方能避免在資料外洩時才開始「補破網」。由於歐盟的個資保護規範為現行全球相當嚴格的規範，提早將相關觀念納入，即能夠同時因應各國的隱私法遵議題。

- **安全設計（Security by Design）**

現代化的醫療設備普遍擁有連網功能(且通常能連上對外網路)，因此這些設備也對安全性和隱私有著更高的要求。安全性儼然已成為醫療設備軟體研發過程中的首要風險及責任，由USFDA發布關於管理醫療設備安全性的規範中，強調醫材設備軟體在研發初期就應將安全性納入產品設計，所以在研發週期的早期階段就需要遵循安全性原則，適當的對所涵蓋資產、威脅和安全弱點的定義進行探討，並且評估醫材設備功能中之威脅和安全弱點對使用者/患者中所造成的影響，以及這些威脅與弱點被利用的可能性。「安全性優先」的設計理念，意味著將整合安全性視為軟體開發週期(SDLC)中的首要考量

此外，在設計產品時建議採用可更新的軟韌體，以迅速因應新出現的問題；需注意的是，在產品進行維護和改版時，安全性仍然是一個持續性的目標，新出現的安全性弱點和威脅也需要以新一代的方案回饋到系統設計中。

- **App檢測服務與IoT檢測**

行動醫療產品設計上，App是極重要的一個元件，不乏惡意程式及個人資料侵害威脅，未來企業勢必將面臨更多行動應用App的安全風險與衝擊。建議企業除了定期執行行動應用App資安檢測作業外，應進一步提早針對行動應用App開發生命週期、委外安全開發管理要求及偽冒App之追蹤管理進行完善規範及評估。

另外，若智慧醫療產品本身採用了感測器有關的IoT技術，也可能要注意是否同時開啟了駭客攻擊的大門。如有疑慮，建議應透過開發安全評估、設備安全檢測等方法確認是否有潛在的風險。

- **國際隱私法規遵循與保護管理**

由於各國隱私法規皆有不同，針對產品預定申請上市的地點，應注意隱私法規的變動，而針對產品與服務模式本身，應該要盤點個資蒐集、處理與利用等生命循環內的流程及管理機制，並且搭配隱私衝擊分析，確定可能造成違法或不安全的情況已充分解決。

- **資訊安全管理**

資訊科技應用除了帶來效益，也會帶來風險，由於資訊架構內牽涉網路設計、作業系統、資料庫、應用程式之結構、存取安全以及技術性參數，若未能充分檢視與確認，可能產生資安漏洞而遭受攻擊或惡意破壞。另外，企業運用雲端環境提供相關服務的可能性日增，雲端相關安全性的評估管理也是重要的環節。

- **個資去識別化管理**

「去識別化」係指透過一定程序的處理，使個人資料不再具有直接或間接識別性，以充份保障個人資料及隱私權，增進互信基礎，並提昇資料運用的價值。實務上同一資料集會採用多項方法進行去識別化處理，當個人資料經由去識別化處理後，則有心入侵者即使取得資料亦無從判斷，即使資料遭竊取亦能降低對當事人隱私之侵害。因此若業者發展的服務中預期蒐集大量的資料，且有想要與其他合作對象發展相關應用時，應當運用去識別化之技術，並同時建立治理框架、風險驗證機制，以強化現行隱私資料保護之強度。

其他策略風險面之因應

- **委外風險管理**

當進行醫材數位化轉型時，可能需要引入新的技術、新的合作夥伴，而且過程中資料的傳遞、存放也可能直接應用資通訊廠商的解決方案。無論是何種形式的委外，都必須考慮雙方責任的分配，資訊安全相關控制（營業秘密、隱私資料處理等）、營運模式的合規與營運能力的持續性等問題。在美國可能也會要求服務供應商必須提供SOC（Service Organization Controls）Type 2 Report，以說明服務機構在資安與隱私上的控制確

實有效。若對於合作對象的風險管理能力有所擔憂，應加以評估，並適度於契約中針對高風險情境考慮納入查核權力。

- **遵循／合規管理**

生技醫療行業屬於高度法規監管類型的行業，而且隨著新的營運模式生成，各國法規與要求也與時俱進。產品如為海外銷售，更是需要當地市場的法規變化。針對智慧醫療轉型下產生的新營運模式，建議應事先籌設專責單位，以及辨識、評估、追蹤法規的機制，並轉換成為內部控制與查檢機制，以確保持續合規。

- **危機預防管理**

目前生醫產品使用上若發生有不良反應或可能傷害使用者的情況，大多適用既有醫藥、醫材不良品、不良反應事件通報規範。由於智慧醫療涵蓋資訊科技元素，針對產品或服務是否產生以往未評估過的風險情境，造成在通報、處置、回收、利害關係人溝通等需要通盤考慮，應加以評估，有必要可應用演練來了解措施上的不足。

隨時關注法規，提前防範風險

醫療與醫材運用資訊科技進行數位轉型，已是趨勢所在。各家業者多已經投入資源開發商機，並且在現行法規架構下尋求可獲利的模式。為了讓投資能夠更加成功，規劃數位轉型藍圖，並引入生態圈的觀念，尋找合適的合作模式，穩定成長；從使用者(病患)為中心提供產品及服務，以取得市場的認可。又由於資訊科技本身帶來的風險，對於業者而言，台灣企業更要注意國際標準、各國法令法規的變化，以調整產品發展策略以及並強化營運、科技以及委外風險控管能力，在發展獲利模式的同時，也能降低潛在風險，提高成功機率。

參考資料

1. Deloitte (2017), “2017 global life sciences outlook”
2. Deloitte (2016), “Will patients and caregivers embrace technology-enabled health care?”
3. Deloitte (2017), “Value of patient experience: Hospitals with higher patient experience scores have higher clinical quality.”
4. Deloitte (2015) , “Smart Cities How rapid advances in technology are reshaping our economy and society.”
5. Deloitte (2017), “The digital hospital of the future: In 10 years, technology may change the face of global health care delivery.”
6. ISO (2016), “ISO-13485：2016 Medical devices — Quality management systems — Requirements for regulatory purposes”
7. ISO (2017), “ISO-80002-2：2017 Medical device software -- Part 2: Validation of software for medical device quality systems”
8. ISO(2006), “IEC 62304：2006 Medical device software -- Software life cycle processes”
9. Digitimes (2017). “避免醫療疏失 提升醫療品質 智慧醫院勢在必行”.Retrieved from：http://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000399544_o9h4cvw55v46qg3s9lrgm
10. Healthdata managment (2017). “FDA approves digital pill that tracks patient compliance”. Retrieved from ：https://www.healthdatamanagement.com/news/fda-approves-digital-pill-that-tracks-patient-compliance
11. Stefaan Callens (2016). “The EU legal framework on e-health”. Retrieved from ：http://www.euro.who.int/__data/assets/pdf_file/0008/138185/E94886_ch13.pdf?ua=1
12. DLA Piper LLP (2017). “Wearable technology and the new EU Regulations on medical devices.” Retrieved from ：https://www.lexology.com/library/detail.aspx?g=e16aa72e-254e-4338-8107-372392a45ec3
13. 科技新報 (2017). “FDA 頒布突破性醫材指引與新 510(k) 指引，加速創新醫材上市.” Retrieved from :https://technews.tw/2017/10/30/fda-510k-guidance/
14. 科技新報 (2017). “歐盟醫療器材法規重大更新，衝擊醫材廠商布局.” Retrieved from ：http://technews.tw/2017/08/03/mdr-medical-equipment-manufacturers/
15. 泛科學(2017).“2016年美國醫療器材五大召回事件” .Retrieved from：http://pansci.asia/archives/121835
16. Inside 硬塞的網路趨勢觀察 (2017). “由於資安漏洞，美國 FDA 召回近 50 萬心律調節器”. Retrieved from ：https://www.inside.com.tw/2017/09/03/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

聯絡我們

作者

吳佳翰 執行副總經理Chia-han Wu
生技醫療產業 風險諮詢服務負責人
chiahwu@deloitte.com.tw

許梅君 協理Mavis Hsu
風險諮詢服務
mavismhsu@deloitte.com.tw

舒世明 副總經理Morgan Shu
風險諮詢服務
morgansshu@deloitte.com.tw

李介文 協理Cathy Lee
風險諮詢服務
cathyclee@deloitte.com.tw

溫紹群 執行副總經理Rick Wen
風險諮詢服務
rickswen@deloitte.com.tw

陳鴻棋 協理 Chris Chen
風險諮詢服務
chrisachen@deloitte.com.tw

另外特別感謝蔡怡華副理、黃彥閔副理、黃建勛副理、徐渝婷資深顧問、李泠葭顧問在本次報告中的協助與貢獻。

勤業眾信生技醫療產業團隊

虞成全 會計師 Robert Yu
生技醫療產業負責人
royu@deloitte.com.tw

黃毅民 會計師Ian Huang
農業生技產業北區負責人
iahuang@deloitte.com.tw

苗德荃 副總經理Alvain Miao
管理顧問服務
alvainmiao@deloitte.com.tw

簡明彥 會計師Steven Chien
醫療器材產業負責人
stechien@deloitte.com.tw

陳惠明 會計師Thomas Chen
稅務服務
thomaschen@deloitte.com.tw

黃詩芳 Shevon Huang
生技醫療產業專案經理
shhuang@deloitte.com.tw

龔則立 會計師 Jerry Gung
醫療照護產業負責人
jerrygung@deloitte.com.tw

潘家涓 執行副總經理Maggie Pan
財務顧問服務
mpan@deloitte.com.tw

許瑞軒 會計師Stephen Hsu
農業生技產業南區負責人
stehsu@deloitte.com.tw

吳佳翰 執行副總經理Chia-han Wu
風險諮詢服務
chiahwu@deloitte.com.tw

專案聯絡窗口

黃詩芳 Shevon Huang
生技醫療產業專案經理
shhuang@deloitte.com.tw

關於德勤全球

Deloitte ("德勤") 泛指德勤有限公司 (一家根據英國法律組成的私人擔保有限公司，以下稱德勤有限公司("DTTL"))，以及其一家或多家會員所。每一個會員所均為具有獨立法律地位之法律實體。德勤有限公司 (亦稱"德勤全球") 並不向客戶提供服務。請參閱 www.deloitte.com/about 中有關德勤有限公司及其會員所法律結構的詳細描述。德勤為各行各業之上市及非上市客戶提供審計、稅務、風險諮詢、管理顧問及財務顧問服務。德勤聯盟遍及全球逾150個國家，憑藉其世界一流和優質專業服務，為客戶提供應對其最複雜業務挑戰所需之深入見解。德勤約220,000 名專業人士致力於追求卓越，樹立典範。

關於勤業眾信

勤業眾信 (Deloitte & Touche) 係指德勤有限公司 (Deloitte Touche Tohmatsu Limited) 之會員，其成員包括勤業眾信聯合會計師事務所、勤業眾信管理顧問股份有限公司、勤業眾信財稅顧問股份有限公司、勤業眾信風險管理諮詢股份有限公司、德勤財務顧問股份有限公司、德勤不動產顧問股份有限公司、及德勤商務法律事務所。勤業眾信以卓越的客戶服務、優秀的人才、完善的訓練及嚴謹的查核於業界享有良好聲譽。透過德勤有限公司之資源，提供客戶全球化的服務，包括赴海外上市或籌集資金、海外企業回台掛牌、中國大陸及東協投資等。

本出版物係依一般性資訊編寫而成，僅供讀者參考之用。德勤有限公司、會員所及其關聯機構(統稱"德勤聯盟")不因本出版物而被視為對任何人提供專業意見或服務。對信賴本出版物而導致損失之任何人，德勤聯盟之任一個體均不對其損失負任何責任。

© 2017 勤業眾信版權所有 保留一切權利