「智慧醫療與資料科學研究倫理與法律」紀要（上）

～臺大醫院倫理中心研究倫理研習會

整理 / 臺大醫院倫理中心 蔡佩璇、戴君芳

壹、前言

2023 年 12 月 8 日，臺大醫院於兒醫大樓 B1 講堂舉辦「智慧醫療與資料科學研究倫理與法律」研習會，邀請多位在醫療倫理及法律領域的重量級專家學者，就「智慧醫療研發趨勢與倫理考量」、「省思智慧醫療應有之法制典範革新」、「層級化的生醫個資利用法制」、「動態同意之實務與法律」、「資料科學研究之倫理審查思維」等議題進行研討。當天特別敬邀幾位貴賓開場致詞，為活動增添不少光彩。

首先，臺大醫院吳明賢院長開場時引用《史記·太史公自序》中的名言：「禮禁未然之前，法施已然之後」，強調倫理是在事情發生前需遵循的原則，包括不傷害、行善、正義及公平，而法律則是最後的防線。他指出，在大數據和人工智慧時代，醫療領域對於倫理和法律的新規範需求尤為迫切，因為醫療直接關係到人體健康和生命。科技應用於醫療領域，只要有適當的倫理和法律規範，不僅可以妥善照護病人、減少醫護人員的壓力，還能提升效率。院長期望通過此次研習會，讓研究人員在了解倫理與法律規範的基礎上，擁抱新科技並解決隨之而來的問題。

臺大醫院高淑芬副院長為督導研究倫理業務，她在接續致詞中指出，隨著智慧醫療的發展，醫療資料的獲取和應用愈加重要，無論是語言 AI 還是生成式 AI，都在處理大量資料方面發揮了重要作用。雖然希望在智慧醫療的協助下，能讓醫療品質和流程更好，但智慧醫療發展也產生了一些疑慮，如是否影響病人隱私，或協助處理的資料被誤用等。因此，此次研習會的主題相當及時且必要，對於現今醫療界及研究人員都是非常重視的議題。

倫理中心蔡甫昌主任為此次活動其中主辦單位，致詞中他提到智慧醫療與資料科學之研究隨著資訊科學家、數學家、電腦工程師及醫學專家共同投入，迅速發展應用。迎接智慧醫療新科技便要面對新產生的科技倫理，這有趣的界面結合臨床照護程序，讓「醫療倫理」與「科技倫理」進行了整合。他強調，本次研習會同時探討了科技倫理、醫療倫理及倫理審查等多個面向，以共同促進醫學進步為目標，而此次參與研習者不僅有研究團隊，還包括研究倫理委員會委員，在審查過程中多應了解科技進展，並理解科技應用於人體同時如何進行受試者保護。

以下紀要先就此次研習會中的「智慧醫療研發趨勢與倫理考量」及「省思智慧醫療應有之法制典範革新」兩個議題進行整理，業經講者確認內容，提供給讀者參考。

貳、智慧醫療研發趨勢與倫理考量：演講者臺大醫院急診醫學部醫師、臺大醫院智慧醫療中心副主任 李建璋教授

醫院的醫療照護程序經由資訊系統生成資料，進而運用科技將行為模式、處方模式、診斷模式等記錄下來，形成神經網路以捕捉資料的模式記憶，並依循此模式進行預測，這即是人工智慧的本質。Medical AI (醫療人工智慧) 具有其特殊性，除了使用結構化資料，還包括生理訊號、影像、聲音等多種資料模型。在目前的研發領域中，人工智慧的發展可歸納為六大趨勢，簡述如下：

第一種趨勢：從單點學習到聯邦式學習 (From Single Site Training to Joint Training)

傳統人工智慧需將影像進行個別標註後建立一個模型，耗費大量人力，且面臨諸多挑戰，如資料樣本數不足、各家醫療院所資料異質性、資料隨時間變動、大量資料攜出之隱私保護與使用目的之控管等。為解決這些困境，聯邦式學習應運而生。例如，多家醫院可共同協議建立一個模型，原本需要由各家醫院各自提出相關資料共同合作完成標註，再進行模型建立；現僅需各醫院各自建立一模型，再將如三家醫院模型放置雲端系統，統整資料、調整參數，找出最適合三家醫院的平衡表現，形成最優模型。

聯邦式學習進一步發展為三種：

1. **垂直聯邦學習 (Vertical Federated Learning)**：將不同項目的標註分工給不同單位，例如腹部影像模型，A 醫院負責肝臟，B 醫院負責脾臟，C 醫院負責胰臟，然後透過聯邦式學習整合，即可形成一個完整的腹部影像模組。
2. **水平聯邦學習 (Horizontal Federated Learning)**：讓同一病人在不同醫院的歷程可直接串連，無需再由醫院調取資料，例如病人在社區醫院及醫學中心接受不同階段照護，即可透過此模式讓兩家醫院合作直接串聯。
3. **聯邦遷移學習 (Federated Transfer Learning)**：例如較小規模的分院數據有限，總院可先將資料建立模型後，再轉移至分院進行學習，最後分院將學習結果反饋給總院。雖為聯邦學習，但這些方式仍需攜出一小部分資料進行串聯比對，從而實現橫向及垂直整合。

第二種趨勢：從單一模態到多模態預測 (From Mono-Modal to Multi-Modal Prediction)

此方法利用機器學習架構，讓電腦在影像上打分數，另外也在結構化資料上打分數，兩個分數統合後進行資料預測，呈現多種不同狀態整合預測。例如，在 COVID-19 疫情期間，全球有 250 多個模型被發表用來預測 COVID-19 死亡率。為突破現有研究現況，發現目前並無融合影像及結構化資料的方法。因此在機器學習架構下，可以讓電腦先對影像打一個分數，再對結構化資料打一個分數，將兩個分數統合起來預測死亡率，此方法被證明比目前任何已發表的 COVID-19 預測死亡率的方法都要精確。

多種不同狀態整合預測需進行模型融合。模型融合可分為幾種方式：

1. **Late Fusion**：結合結構化資料預測及電腦資料預測的預測結果。
2. **Early Fusion**：將早期影像如同實驗室數據、病史，集中為一個特徵，合併做成一個模型。
3. **Joint Fusion**：將影像轉換為文字描述作為基準後，再進行整合。
4. **Common Space Fusion**：不論結構化資料或影像資料，先整合在一個共同

空間，使用相同的矩陣做資料整合和分類。以上技術皆可讓不同資料進行整合，獲取最佳權重。

第三種趨勢：從海量資料學習到少樣本學習 (From Voluminous Data Learning to Few-Shot Learning)

數位孿生 (Digital Twin) 原出自於工業應用，當時要模擬飛機飛行時，需要在風洞中測試風阻係數，以研究如何讓飛機更輕、更省油，且風阻係數更佳。傳統方式需要使用黏土、木頭等建立飛機模型，並在風洞裏測試；現在可將風洞係數、不同條件環境溫度等數位化後進行模擬，此種將現實世界產品數位化後進行環境模擬測試結果，即為數位孿生。在醫藥界可用於模擬藥物在人體中代謝狀況、模擬施打藥劑後影像等。例如，腎功能不全的病人不能施打電腦斷層掃描檢查的顯影劑，數位孿生可模擬出病人在各種條件下施打顯影劑後的結果，此應用令人非常振奮。

第四個趨勢：從單一病灶檢測到多重病灶檢測 (From Single Lesion Detection to Multiple Lesion Detection)

過去在電腦斷層中，欲檢視腫瘤治療後是否改善，建立的模型在真實世界中往往會失真。例如糖尿病視網膜病變，收集該疾病病人與健康人的資料進行分析，電腦學習後可能已有 99% 的準確率可分析疾病，但放到真實情境時，病人可能還有其他如青光眼、高血壓等，電腦無法識別，成效因此下降，需要如眼科醫師般具備豐富經驗來分辨眼睛疾病的影像特徵。舉例來說，國外影像專家 Ronald Summers 所帶領的團隊，不藏私地公開分享包含良性、惡性、感染等已註記的 10 萬筆胸部 X 光影像，再由其他專家進行標註約 3.2 萬份，當使用者在此基礎模型中輸入影像資料後，即會顯示該影像的所有問題標註，這即為 Deep Lesion。這個基於 10 萬筆影像訓練出的基礎模型，再以少量影像微調整，即可形成完整的模型。由此觀之，電腦視覺模型已進入「博觀而約取，厚積而薄發」的階段。

第五個趨勢：從被監督學習到自我監督學習 (From Supervised to Self-Supervised Learning)

傳統的監督學習方式需要將內容標註才能讓電腦學習；而自我監督學習則是由

電腦自行生成問題，自行判讀及進行分析與學習。最新的方法為對比學習 (Contrastive Learning)，即在學習過程中給予一個正樣本 (例如貓)，再給予一個負樣本 (例如狗)，電腦學的不僅是辨別貓或狗，而是會找到一組參數將狗和貓區分得最開。這對比學習可以用於自我監督學習或傳統技術上，能夠非常快速地學習。這趨勢亦為近期快速發展的技術，預見擬人化機器人技術也將迅速發展。

第六個趨勢：從預測到生成式人工智慧 (From Predictive to Generative AI)

現今生成式 AI 影響最大的莫過於 ChatGPT，其本質為超級克漏字填詞機，僅依照前後文填上最可能的文字，並無法真正理解文章內容。現今突然爆紅的主要原因即是利用了 Transformer 架構技術，這技術讓電腦能閱讀整篇文章，甚至數千篇資訊，然後做出更為準確的預測答案，彷彿杜甫詩句「讀書破萬卷，下筆如有神」。目前全世界僅有 OpenAI 公司擁有此模型，若要使用 ChatGPT，就需將資料貢獻出去。然而，競爭對手 Meta 公司則開發規模較小的 LLaMA (Large Language Model Meta AI 模型)，並公開釋出供大眾使用。例如，可下載 LLaMA 模型並搭配院內醫療資料，便可建構機構內部的模型。在使用前可進行知識提煉 (Knowledge Distillation) 過程，將問題提交給 ChatGPT 回答，然後讓模型學習如何模仿 ChatGPT 的回答，如此可快速提升模型效能。目前如同中央集權與地方分權，競爭態勢尚未決定，勝負難以預料。

AI 的風險與管制原則

AI 進步速度迅速，但也可能產生一些疑慮，例如資料外流風險、外流後被他人利用的風險，以及演算法正確性等問題。世界衛生組織公布的《Regulatory Considerations on AI for Health》提出任何機構管制 AI 時應遵循以下六項原則：

1. **透明度與文件化 (Transparency and Documentation)**：使用的資料、訓練的演算法、得到的模型在公開使用時必須公開透明。
2. **風險管理 (Risk Management)**：需事先規劃 AI 可能發生的誤差及性能下架的管理機制。
3. **預期用途及分析與臨床驗證 (Intended Use and Analytical and Clinical Validation)**：必須清楚且符合訓練的目標及適應症。

4. **資料品質 (Data Quality)**：除了演算法外，亦需檢查資料品質是否符合原則。
5. **隱私與資料保護 (Privacy and Data Protection)**：安裝 AI 後不能開後門將醫院的資料另存，且資料不能用於運算以外的其他用途。
6. **參與與合作 (Engagement and Collaboration)**：所有監管機構、病人、醫療專業人員、業務相關代表及政府夥伴之間都要進行合作，以確保產品和服務在其整個生命週期符合監管要求。

人工智慧技術演進是一種人類內在觀照自我學習的原理，並將之體現於演算法的過程中。資料科學家以方程式演算出這些原理，研究者若能理解這些原理，便可設計出優良的人工智慧研究，並在開發人工智慧與應用於智慧醫療時，應遵循負責任與可信賴的人工智慧原則。

參、省思智慧醫療應有之法制典範革新：演講者臺北醫學大學人文暨社會科學院副院長李崇僖教授

現今法律制度的典範是在舊的科技底下形成，雖目前運行適當，但有新科技產生時，則有新的課題及挑戰，若法治典範未依新科技方式改變，新科技將不易發展、轉型及落實。

智慧醫療帶動的規範革新概要分為四心：「以病人為中心」、「以軟體當核心」、「以資料做創新」、「以專業固信心」。

第一個「以病人為中心」，希望能透過智慧醫療，記載及分析病人個人化資料後，為病人進行最佳治療之個人化醫療，且若以病人為中心，則不僅以醫院場域為限，病人在社區、診所，皆可得到連貫性醫療服務。這部分會涉及不特定場域的醫療活動、實施遠距醫療包含數位健康模式，甚至將服務醫療專業延伸至預防保健、照護等。在以病人為中心的相關法制典範會帶來哪些調整？例如遠距醫療在 2023 年初開始討論，2024 年通訊診察治療辦法將有大幅修正並正式公告，將會衝擊醫療行業，需思考臺灣長期以來健保法規規定的醫療分級制度、家庭醫師如何落實，以及如何讓民眾獲得連貫性的醫療照護服務等。進一步達到預防保健連動性，未來若希望做到數位健康模式，則期望民眾願意在預防保健部分投入費用，數位健康模

式方有意義。因此需思考整體制度的設計制度，例如給予健保保費折扣等誘因。

在數位健康部分，指病人不僅是在醫院掛號後才產生醫病關係，醫療照護成為長期性的關係，但這需思考醫療照護責任界定到何時，過去是在病人進出醫院這段時間，但未來，如何去判斷醫療疏失發生的時間、地點及責任歸屬，未來均會需要進行討論。

第二個「以軟體當核心」，機器學習 AI 因在臨床場域使用時會因資料輸入而改變其演算的模型，需要監控機制，機器學習式醫材如何動態監管，舉例美國國會授權 FDA，針對機器學習軟體做彈性化審查，故 FDA 於 2023 年 4 月發布 *Predetermined Change Control Plans for Machine Learning-Enabled Medical Devices: Guiding Principles*，若有醫療軟體申請許可證時，須附上預估臨床應用時會有的變化，以及須如何監控變化，若未來實際使用時其變化是否在原預期範圍內則不用再送審。若超過預期變化範圍，則須重新送 FDA 進行審查，目前臺灣尚未有此制度。以軟體當核心的醫療科技，審查機制開始朝向事後監控，包括軟體後續資料合法性、監控等。此方式若在臺灣使用，醫療機構勢必須將資料提供產品廠商進行分析及監控。

機器學習式醫材如何動態監管，舉例德國已於 2019 年制定數位醫療應用法律，數位療法即是使用 APP 類產品，替代醫師提供治療，德國藥政主管機關針對申請之廠商產品進行安全及有效性評估後，即分級提供給付，持續監測一年後來決定是否正式納入給付清單。因此應用上需考量臨床效益如何評估。在人機協作中，人是在整個機器運作循環的角色，人可以更好的控管系統，但也可能干擾機器運作，因此亦須考量如何人機協作。

第三個「以資料做創新」，軟體表現建立在資料品質，在軟體進行機器學習時，訓練數據的品質、持續機器學習的品質，皆以資料驅動型創新為基礎。目前健康資料缺乏整合利用機制，例如，在日本，有次世代醫療基盤法，民眾在不同醫院就醫，若要獲得精準之醫療資料，須將醫療資料交至一個單位，該單位具有個資，可將不同醫院、不同資料整合及串接後，提供研究者匿名使用。目前臺灣並無此法制，但因資料是創新的基礎，故仍設立專法，並須朝向建立資料交易機制，目前醫院不願提供資料交給外部廠商有兩種考量，一為法律責任，依照醫療法規定，須保

護病患隱私，二為病歷資料價值性高，該如何建立資料交易機制，目前尚無法律保障此權益及交易。

第四個「以專業固信心」，最終不希望醫療專業被資訊科技取代，醫療專業未來與 AI 進行人機協作時，讓專業團隊對 AI 所分析出來之資訊可應用性、如何使用等進行把關，以及評估新科技導入後，醫療責任將會產生哪種改變；過去醫療法規範透過案例所制定規則及標準，因為科技進步而需再次改變，需從產品開發到最後醫療責任，了解責任之界定及相關問題，才有可能透過連貫性處理智慧醫療落地應用的問題。

醫護人員養成須重視人機協作能力，在醫護人員訓練過程中，須能妥善了解、操作機器；最重要的是需要釐清醫療責任與產品責任問題，兩者之責任該如何界定，誰該負責？醫療有了 AI 輔助情況，醫療人員多了一個參考資料，但若發生醫療事故，這參考資料可能成為另一種證據。若機器提出警訊，但醫療人員未採用機器所提出的建議，對醫療人員而言反而更容易構成疏失，對醫療人員而言，責任反而提高。在醫療法第 82 條的醫療責任，因故意或違反醫療上必要之注意義務，且逾越合理臨床專業裁量需負損害賠償責任，合理臨床專業裁量是希望醫師現場所做的判斷在事後受到一定程度的尊重，但隨著醫療科技發展進步，合理臨床專業裁量的空間可能會縮小，醫師提抗辯、舉證的責任會提高，也許醫療法本身亦須因應醫療科技發展思考適當的標準。