人工智慧醫療實務應用下之法制問題探討

胡峰賓*
翁紹仁**

壹、前言

近年來，台灣醫學中心之智慧醫療發展，已顯其長足進步與高度潛力[1]，遂成醫療體系轉型之重要推手。憑藉台灣完善之健保資料庫與先進資訊科技基礎設施，智慧醫療於疾病之診斷、治療、預防與長期管理等面向，持續推陳出新。尤在醫療影像識別、疾病風險預測與個人化醫療等領域，屢獲具體成果。其例尤著者，如中國醫藥大學附設醫院於AI輔助診斷之應用，成效斐然，特別是在醫學影像分析方面，藉由導入AI系統協助判讀X光、CT與MRI影像，使肺癌、乳腺癌與腦中風之早期診斷準確率得以提升，分析時間顯著縮短，亦有效減輕臨床醫師之工作負荷。復如「智抗菌i.A.M.S平台」，整合AI與資訊科技，強化抗菌治療之精準性，其內含智能抗藥性細菌快速預測系統、AI自動敗血症輔助診斷系統、個人化抗菌圖譜及抗生素治療輔助決策系統，使傳統抗藥性細菌分析時間由72小時縮短至1小時，醫療團隊得以即時為感染病人選擇正確用藥，病人存活率並顯著提升23.7%。[2]

此外，多家醫學中心成功運用人工智慧（AI）技術，建置輔助診斷系統，有效促進癌症與心血管疾病之早期發現，並提高診斷準確性。[3]COVID-19疫情之爆發，更加速遠距

＊本文作者係執業律師，臺灣大學法律所博士，法國Aix-Marseille大學法律碩士，中國醫藥大學中醫系碩士，北京大學醫學部博士班。
＊＊本文作者係醫療系統聯盟理事長，東海大學跨域創新學院院長，東海大學工業工程與經營資訊學系教授。

註1：林宛儀、林勤真、鍾翰其、洪聖惠、饒孝先、郭惠雯、徐珮嘉、王拔群（2023），〈2022年臺灣智慧醫療發展現況調查〉，《醫療品質雜誌》，17(1)，第6-12頁。
https://doi.org/10.53106/199457952023011701001

註2：中國醫藥大學附設醫院，大數據與人工智慧發展。
https://www.cmuh.cmu.edu.tw/CMUHPages/BigDataAndAI

註3：陳韋成、陳蒼潔、洪千惠、張榕浚、王毓駿（2022），〈參與「醫療科技問題與病人安全風險學習平台（ITPS）」經驗分享〉，《醫療品質雜誌》，16(4)，第16-20頁。
https://doi.org/10.53106/199457952022071604003

醫療、雲端藥歷與視訊門診等應用之普及。[4]智慧遠距醫療之推廣，亦突破地理限制，尤對偏鄉或醫療資源匱乏地區助益甚鉅，使當地居民亦能獲得即時而有效之醫療服務。臺中榮民總醫院於2022年成立「遠距照護中心」，整合高齡醫學、心血管醫學、神經醫學、家庭醫學與資訊部門等多方專業，共同推動遠距醫療之發展。該中心結合人工智慧、行動通訊技術、數位裝置及資通訊科技之應用，提供24小時遠距醫療服務，專注於視訊診療、遠程監控與健康諮詢，顯著縮短病人就醫之實際距離，並提升醫療服務之可近性。[5]然台灣推動遠距醫療與會診之主要瓶頸，仍在於現行《醫師法》第11條所定「親自診察」之法律限制。該規範長期以實體面診為原則，致結合資通訊技術（ICT）之非接觸式醫療，其合法性迭遭質疑。爰此，衛福部於113年7月1日修正《通訊診察治療辦法》，就急性住院出院後照護、在宅醫療等5項特殊情境提供例外規範[6]，重新詮釋「親自診察」之內涵。惟遠距醫療涉及高度敏感之健康資料傳輸與儲存，如何在遵循《個人資料保護法》之前提下，防杜個資外洩風險，仍為智慧醫療轉型不可迴避之關鍵課題。就產業層面言之，臺灣生技醫療產業近年積極結合人工智慧（AI）與機器學習（ML）技術，以加速新藥研發流程並有效降低其高昂成本，藉以回應傳統新藥開發動輒耗費鉅資、歷時10餘年之結構性困境，並進一步推動精準醫療之廣泛實踐。是以，AI已非僅止於輔助工具，而實為生醫產業創新模式之關鍵引擎。例如2021年美國知名生技創投機構Flagship Pioneering所孵化之Generate：Biomedicines，建構一整合式技術平台，將蛋白質科學之專業知識、結構生物學中既有之蛋白質與勝肽資料，與機器學習模型相結合，得以快速生成各類疾病治療所需之抗體、酵素、勝肽，以及細胞與基因治療方案，使整體新藥研發流程大幅縮短，甚至可於兩年內完成[7]，顯著顛覆既有藥物研發之時間尺度。

復次藉由人工智慧分析海量基因體資料與臨床病歷資訊，臨床醫師得以為病患量身訂製更為精細之治療計畫，從而提升整體治療

註4：廖熏香、饒孝先、徐珮嘉、王拔群（2019），〈醫策會智慧醫院架構與評量〉，《醫療品質雜誌》，13(2)，第20-23頁。
https://www.airitilibrary.com/Article/Detail? DocID=a0000532-201903-201905020029-201905020029-20-23

註5：臺中榮民總醫院遠距醫療中心（2024），遠距醫療中心 / 關於我們 / 使命沿革。
https://www.vghtc.gov.tw/UnitPage/UnitContentView?WebMenuID=65c01262-21bf-44ae-aab1-d175e890eaeb&UnitDefaultTemplate=1

註6：衛生福利部醫事司（2024），「衛福部發布修正通訊診察治療辦法提升醫療近便性」，衛生福利部新聞，
https://www.mohw.gov.tw/cp-16-77322-1.html

註7：新創幫（2024），解析：新創技術。
https://innoaward.taiwan-healthcare.org/news_detail.php?REFDOCID=0slblbhg1zctjd41&REFDOCTYPID=0lmxluatpgjqd6bo

成效。中國醫藥大學附設醫院所設之基因體醫學中心，整合患者之基因數據與臨床表徵，廣泛運用AI於基因組學分析，其應用涵蓋次世代定序資料判讀、基因型插補以及多基因風險評估等，藉以辨識致病基因或潛在危險因子，並據此發展個人化治療策略，不僅療效顯著提升，亦有助於減少不必要之藥物副作用（見圖1）。

又智慧醫療應用之日益深化，促使醫療流程趨於數據化與標準化，進一步提升整體醫療品質與作業效率。高雄榮民總醫院成立研創暨智慧醫療中心，協助院方推動智慧型醫院之轉型，專責探索並導入前瞻科技，持續創新臨床服務模式，並優化資訊系統，以強化醫療品質之穩定與安全。其所開發之抗生素智能管理系統，建立國內首見之抗生素升階與降階警示機制，並結合品質管理方法，從劑量自動帶入、藥師審核平台至用藥監測[8]之整體流程，系統性抑制多重抗藥性菌株之發生。

該系統不僅提升抗生素使用之適當性與效率，使病患得以及時獲取有效治療，並於實務運作中顯示，每年可為醫院節省隔離衣等感染管制相關成本約新臺幣七十餘萬元。憑藉智能化抗生素管理之成效，高雄榮民總醫院遂於2022年成為南臺灣唯一通過感染管制與抗生素管理雙重認證之醫療機構，足證智慧醫療於產業與臨床交會處之實質價值。

臺灣近年致力於結合物聯網（IoT）與穿戴式生理監測設備，建構疾病預警與長期健康管理體系，使醫療介入得以前移於疾病發作之前，不僅有助於提升患者生活品質，亦能有效紓解醫療量能之結構性壓力。復以國家級數據平台之整合運用，彙集跨院、跨域之健康資訊，更使公共衛生決策得以建立於科學證據與即時數據之基礎上，其治理精準性與前瞻性，因而大為增強。

圖1：中國醫藥大學附設醫院發展全人照護之精準醫學架構圖

註8：許麗娟（2023），〈抗生素抗性問題嚴重高榮講謹記「四不一要」〉，自由健康網。https://health.ltn.com.tw/article/breakingnews/4210972

以林口長庚紀念醫院為例，該院自2014年獲頒全臺首座「智慧醫院標章」以來，旋於2017年全面啟動智能化轉型；2018年復成立「AI核心實驗室」，作為院內技術研發與應用之樞紐。其透過巨量臨床資料庫與深度學習架構，陸續開發多元臨床診斷模型，並將電腦視覺、自然語言處理及商業智慧（BI）系統導入醫療管理實務，實現醫療數據之視覺化監控與自動化蒐集[9]，顯著提升決策效率與臨床管理品質。

又於金融科技之領域，銀行與保險機構亦開始運用人工智慧進行風險評估、理賠審核與客戶服務，間接促進醫療保險、健康管理與金融服務之數位化整合，形塑醫療與金融跨域融合之新型態。總觀而言，臺灣智慧醫療之發展，係在政府政策支持、醫療體系深化、產業創新動能與科技應用成熟等多重因素交互推動下，已展現強勁且持續之成長勢能。展望未來，倘能配合持續之科技革新與制度完善，臺灣有望成為亞洲智慧醫療之重要樞紐，並對全球醫療科技之進步，發揮關鍵影響力。

然而，智慧醫療之深化，亦引發根本性之法律追問：人工智慧之法律性質究竟為何？醫師與病患能否真正理解，並進而信任AI之判斷結果？就現行法制言之，醫療AI尚非法律主體，其法律定位多被歸類為「醫療器材」、「醫療軟體」或「專業輔助工具」，其性質近於高階診斷設備，如MRI或CT影像判讀系統，而非具備判斷自主權之「準醫療人員」。是以，AI所提供之分析結果，於法律上僅具參考地位，最終醫療決策與責任歸屬，仍須由臨床醫師承擔。

然隨深度學習模型日益複雜，其推論過程往往呈現高度不透明，實務上已浮現所謂「理解落差」之問題。多數醫師與病患，難以充分掌握AI判斷之資料來源、推論邏輯與潛在偏誤風險，致使信任基礎不再建築於可理解性之上，而回歸醫師既有之臨床經驗與醫療常規。於此情形下，AI醫療決策之合法性與透明性，遂成為法制不可忽視之課題。

若醫療AI之決策演算法屬「黑箱系統」，致醫師與病患無從理解與檢驗其判斷，則法律上如何課以「可解釋性」與「審查機制」之要求，亦頗值探討。自法律責任與病患權益保護之觀點觀之，要求醫療AI具備一定程度之可解釋性與制度化審查機制，實屬必要之發展方向。所謂可解釋性，並非要求全面揭露演算法之技術細節，而至少應能說明其判斷所依據之關鍵特徵、信心水準及適用範圍與限制，使醫師得以據此行使專業判斷，法院亦得於事後審查時有所依循。

至於審查機制，法制上得考慮要求醫療AI系統於上市前、臨床使用中，及重大版本更新時，接受第三方驗證與持續性監測。此種機制，實可視為「技術化之醫療品質管理制度」，其目的在於於制度層面提前控管風險，而非將潛在責任全然轉嫁於第一線臨床醫師。

準此以觀，現行醫療實務中，多數醫療人

註9：長庚醫療財團法人永續發展（無日期），〈ESG永續資訊──用AI讓醫生留更多時間給病人！林口長庚院長：智慧醫療不是為做而做〉，長庚醫療財團法人官網。
https://webapp.cgmh.org.tw/csr/news-c.aspx?id_seq=E4AMB48001

員對AI之導入與使用，仍存諸多法律疑慮。概其法律風險與爭議，主要可歸納為二：其一，醫療決策錯誤時之責任歸屬問題[10]；其二，資料蒐集、利用與保存所涉及之個人資料保護與隱私權法制問題。[11]此二者，皆為智慧醫療持續發展過程中，亟待透過法律規範與制度設計加以回應之核心議題。

貳、醫療責任歸屬問題

隨人工智慧（AI）自「輔助診斷」而漸進於具「實際診斷」之潛能，醫療體系面臨前所未有之法律挑戰。若AI誤判而致醫療差錯，責任應歸誰？醫師乎、醫院乎、開發商乎、抑或使用者乎？現行法制，能否應對此技術革命之情境？是章將自法律原則、臨床實務及具體案例而論，探討AI醫療之責任框架。

一、核心原則：AI目前僅為「輔助工具」而非法律主體

AI若由輔助診斷進階至實際診斷，若誤判致醫療差錯，其責任當如何歸屬？法律上應由誰負責？是醫師、醫院、開發公司，抑或AI使用者？依現行法制觀之，誤判所生之法律責任，核心仍回歸「醫療行為之決定主體」。於現行法下，AI為輔助工具，非法律主體，無獨立責任能力，原則上不可能由AI本身負責。實務上，責任視具體情境，或歸醫師，或歸醫療機構，或歸開發商。就醫師責任而言，以「是否盡合理專業注意義務」為判準；若醫師過度依賴AI，未行合理檢證，或在顯有疑義時不再確認，或構成醫療過失。醫療機構如於AI系統選用、驗證、教育訓練或流程設計有缺失，亦可能成立管理過失。

然現行醫療責任制度，多建立於「單一醫師—病患」關係之上。面對AI之多方參與（開發商、資料提供者、醫院、醫師），制度顯不足。實務上責任多集中於第一線醫師，致生防衛性醫療，亦或阻礙AI應用之風險。

二、臨床決策衝突：當AI與醫師判斷不一

臨床實務中，如心血管疾病預測或癌症判讀，常見醫師與AI意見相左之情形。若病患依醫師指示治療，而結果不良，法律責任如何？依現行法制，若病患依臨床醫師指示接受治療，而事後發現誤診或治療不良，法律責任仍原則歸醫師。關鍵不在「誰判斷正確」，而在「當時醫師判斷是否符醫療常規及專業水準」。法院多採「事前合理性判斷」，非事後結果論。

若醫師當時有合理理由不採AI結果，例AI

註10：Cross, J. L., Choma, M. A., & Onofrey, J. A. (2024). Bias in medical AI: Implications for clinical decision-making. PLOS Digital Health, 3(11), e0000651. https://doi.org/10.1371/journal.pdig.0000651

註11：Chen, Y., & Esmaeilzadeh, P. (2024). Generative AI in medical practice: In-depth exploration of privacy and security challenges. Journal of Medical Internet Research, 26, e53008. https://doi.org/10.2196/53008

尚未成為醫療常規、模型未經充分驗證、或病患個別情況不符模型條件，即便AI事後證明正確，醫師亦未必構成過失。反之，若AI已廣泛為標準輔助工具，而醫師未說明理由即全然忽視，則或認為違反注意義務。此時，AI「正確性」成為衡量醫師盡責與否之重要參考，然AI不取代醫師為責任主體。

疾病診斷常有多種風險因子，如膀胱癌患者可見血尿、頻尿，危險因子則有家族史、吸菸、咖啡、接觸有機溶劑等。AI可迅速整合上述因素，預測罹病機率。若醫師全信AI預測而誤診、延誤治療，法律上責任仍主要由醫師承擔。蓋醫師被視具專業能力，應能獨立判斷AI結果之合理性，AI無決策權。然若醫師依合理使用指引操作AI，且於資訊揭露、風險說明及專業判斷上無重大疏失，可主張已盡注意義務。

若醫師依TFDA核准醫療AI錯誤判斷而治療，致病患死亡或失能，病患或家屬求償，醫師可否主張「因AI誤判，影響決策」？開發商是否應負產品責任？醫師與開發商之責任如何區分？依現行法制，若誤判源於系統設計缺陷、資料偏誤或未充分揭露限制，開發商可承擔產品責任，病患得求損害賠償；醫師責任則依誤判原因與醫師行為關聯決定。若醫師僅合理使用本有缺陷之AI系統，且無法合理察覺問題，或可符合醫療常規。

三、具體案例分析：AI醫療應用之責任歸屬實證檢討

（一）案例一：低劑量電腦斷層（LDCT）影像判讀歧異與時間落差之法律評價

1.事實情境

病患接受低劑量電腦斷層檢查以進行肺癌篩檢，AI系統於影像中提示疑似高風險病灶。惟臨床醫師綜合當時影像品質、病灶大小及既有醫學常規，認其尚未達立即處置之必要，僅建議定期追蹤。數年後，病患確診肺癌，遂質疑當年未依AI提示進一步處理，是否構成醫療疏失。

2.爭點所在

當AI與醫師判讀結果不一致，且疾病具時間演變性時，是否得以事後發病結果，回溯認定醫師當年違反注意義務？

3.法律評析

依現行醫療責任法制，醫療過失之判斷原則上採「事前合理性標準」，而非「事後結果論」。注意義務之認定應以醫師作成判斷當時之醫療情境，而非疾病最終結果。具體而言，應審酌下列要素：當時影像是否已達一般醫師可合理預見之異常程度；醫師是否依醫療常規提出追蹤、轉介或進一步檢查之建議；AI所示警示是否已明確標示高度惡性風險，而非僅屬模糊提示。

醫師應依專業判斷盡注意義務，又《民法》第184條則明定侵權行為責任需符合「過失存在」之要件。兩者共示：醫療過失之認定，應以「事前合理性標準」為準，即以醫師於當時可合理取得之資訊、現有醫學常規與技術水平為依據，而非單憑事後結果認定。醫師責任應依專業判斷、現有證據及風險評估，而非僅以事後結果追究責任。此為醫療法律責任與倫理責任共通之核心精神，亦可作為我國法院在AI輔助診斷案件中之參考。AI屬高風險醫療器材，其

功能以輔助醫師判斷為主。AI之診斷提示或風險警示，原則上並不取代醫師最終判斷與處置責任。若AI報告已明確提示高風險，但醫師未說明理由即完全忽略，法院或可將該AI提示視為「已存在之警訊」（existing warning），作為衡量醫師注意義務是否履行之證據，然此僅係評估醫師行為合理性之參考。

醫療機構應建立AI判讀結果之內部審核及追蹤機制，包括結果核對、異常標示、後續追蹤建議，符世界衛生組織（World Health Organization, WHO）於2021年6月底公布「人工智慧於健康領域之倫理與治理」（Ethics and governance of artificial intelligence for health）指引中所提透明度、可追蹤性及責任歸屬之原則。此舉可降低醫療爭議風險，並兼顧患者安全與醫師責任防護。[12]

（二）案例二：AKI透析病人使用低血壓預測模型失準之責任歸屬

1.事實情境

於急性腎損傷（AKI）病人之透析過程中，醫療團隊使用「透析中低血壓預測模型（Intradialytic Hypotension Prediction Model）」作為輔助監測工具。然該AI系統未能即時預測低血壓發生，病患於透析中出現休克，並導致嚴重併發症。

2.爭點所在

AI預測失準，是否得作為醫療團隊主張免責之依據？

3.法律評析

在現行法制架構下，AI僅屬輔助監測工具，並不取代既有之生命徵象監控與臨床即時處置流程。醫療團隊仍負有持續觀察與即時介入之基本義務。於此類案件中，通常將檢視：醫療團隊是否仍依標準程序持續監測血壓、心率等生命徵象？

是否因過度信賴AI，而忽略其他臨床警訊？是否仍維持人為監控與即時判斷機制？醫師於臨床中使用AI輔助工具，仍須保持合理專業注意義務（duty of care），不得因AI預測失準而自動免責。醫療團隊仍應依標準操作程序持續監測病患生命徵象，並及時介入。高風險醫療AI僅為輔助，醫師仍須保有人為監控與判斷能力，確保患者安全；若因過度依賴AI而忽略臨床警訊，可能違反注意義務與倫理原則。

是以應審查醫療團隊是否依標準程序監測血壓、心率等生命徵象，未因過度依賴AI忽略臨床警訊，保有足夠的人為判斷與即時處置機制。若醫療團隊合理使用AI，且持續遵循臨床標準流程，縱

註12：醫師應保存決策理由紀錄（decision rationale），包括AI輔助結果、臨床判斷依據及追蹤計畫，以利日後法律爭議時證明注意義務已履行。此亦呼應國際醫療倫理中「專業責任（professional responsibility）」及「可追溯性（accountability）」之要求。鑒於癌症具漸進性與高度不確定性，僅憑多年後之確診結果，尚不足以推定醫師當年判斷即違反注意義務。惟若AI於當時已清楚標示高度惡性風險，而醫師未加說明即完全忽略，亦未安排任何追蹤措施，該AI報告即可能被認定為「已存在之警訊」。

AI預測失準，通常不構成醫療過失；反之，若將AI視為唯一警示，忽略傳統監測，則可能構成過失。至於產品責任部分，依歐盟《醫療器材法規》（Medical Devices Regulation (EU) 2017/745, MDR）.及《人工智慧法案》（AI Act, 2024/1689），若AI系統因設計缺陷、資料偏誤或訓練不足而導致患者傷害，開發商可能須承擔產品責任。

而醫師責任與開發商責任之區分，須依因果關聯與可合理預見性判斷：若醫師已合理使用一個本質上存在缺陷的AI系統，且無法透過其他專業判斷察覺問題，則可主張其符合醫療常規；若醫師忽略臨床警訊，過度依賴AI，即使系統有缺陷，仍可能負過失責任。AI輔助工具之失準不可作為醫師自動免責理由。關鍵在於「醫師是否合理依循現有臨床標準與AI使用指南」，並建立適當人為監控與即時處置流程。此原則符合我國醫療過失之事前合理性標準（非事後結果論），亦呼應國際醫療倫理強調的「責任不可完全轉嫁於AI」。若醫療團隊將AI視為主要甚至唯一之警示來源，而怠於傳統監測與即時處置，縱AI預測失準，仍可能構成醫療過失。原則上，AI系統之失效，並不得作為免責理由。

（三）案例三：腎臟病理AI誤判之模型限制與揭露義務

1.事實情境

AI腎臟病理模型判讀結果為腎絲球腎炎，惟實際病理診斷為微小變化病（Minimal Change Disease）。事後查明，誤判主因在於腎絲球結構近乎正常，且樣本本身具高度侷限性。

2.爭點所在

此類基於模型限制所生之「合理誤判」，是否仍可能有法律責任？

3.法律評析

法律評價之核心，並非在於AI是否可能誤判，而在於其「限制是否已充分揭露」。若模型之適用範圍、樣本限制及誤判風險已於使用說明中明確揭示，且臨床醫師亦知悉須結合臨床表現與其他檢查結果進行判斷，則該誤判風險應屬可接受之醫療不確定性。醫師於使用AI輔助診斷時，仍須保持合理專業注意義務（duty of care），但合理誤判若基於AI模型已揭露之限制，通常應不構成醫療過失。「合理誤判」屬醫療行為之不確定性範疇，核心在於醫師是否已依現有專業知識與合理判斷，適當解讀AI結果並搭配臨床檢查進行判斷。若醫師依AI提示進行必要交叉檢驗，仍發生誤判，應視為可接受之醫療風險。AI屬高風險醫療器材，其功能、限制及潛在誤判風險需明確揭示，若開發商未充分揭露模型適用範圍與誤判風險，病患因合理信賴而受損，開發商可能承擔產品責任，醫師若未遵循使用說明、未搭配必要臨床驗證而導致損害，也可能承擔醫療過失責任。

AI高風險應維持透明度（transparency）與可追蹤性（traceability），使用者（醫師）需知悉工具限制並作專業判斷；醫療機構應建立內部審核流程與決

策紀錄，以降低法律與倫理風險。此外，醫師應依專業判斷執行醫療事務，AI僅屬輔助工具，誤判不應直接歸責於醫師，但醫師有責任確保AI使用符合臨床常規與限制揭露。[13]

（四）案例四：AI輔助判讀結果納入正式報告而未處理之法律效果

1.事實情境

AI於影像判讀中提示病患疑似骨質疏鬆，該結果隨同醫療報告呈現，並可供病患依法申請閱覽。惟醫師原開立檢查之目的並非評估骨質疏鬆，遂未進一步處理，亦未向病患加以說明。

2.爭點所在

當AI結果已納入正式醫療報告，醫師未處理或未說明，是否有法律責任？

3.法律評析

一旦AI輔助判讀結果成為醫療紀錄之一部，即不得認為「不存在」。醫師縱與AI判斷不同，法律上固不禁止，但仍應盡說明與記載義務。醫師雖可依專業判斷與臨床目的決定是否採納AI結果，但仍應保留最低限度的說明或註記，避免未來爭議。若醫師未處理或未說明，該AI判讀可能被法院視為「已存在警訊」，用以衡量醫師是否履行注意義務。

醫療AI高風險工具應保留透明可追蹤之使用記錄，並建立內部審核流程，醫師應向病患提供必要資訊與決策依據，確保知情同意與自主權。依此，AI輔助結果納入報告後，醫師應於臨床上進行必要的說明或記錄，否則可能違反透明度及告知義務。因此，醫師對AI結果的處理，可分為三種情境：第一，合理採納：醫師依AI結果輔助判斷，並進行臨床驗證，屬正常醫療行為；第二，合理忽略：醫師有充分理由認為AI結果不符合臨床情境，需註明理由或保留註解；第三，未處理或隱匿：醫師完全未處理、未註記，可能構成對注意義務及告知義務之違反，AI報告成為日後爭議之不利證據。總結而言，AI輔助判讀納入正式報告後，醫師雖不必完全依其結果行動，但仍須履行基本說明、註記與追蹤義務，以符合法律及醫療倫理要求。若醫師完全未處理、未解釋AI所提示之異常，日後病患發生相關損害，該AI報告即可能被認定為「已存在之警訊」，進而成為未盡告知或追蹤義務之不利證據。

（五）案例五：手術機器人與AI輔助系統之同意義務與責任分流

1.事實情境

手術中使用自動化手術機器人，在前置作業及醫師操作均無明顯疏失之情況

註13：另AI誤判是否構成法律責任，應考量模型是否已揭露適用範圍與誤判限制；醫師是否依合理臨床程序進行判斷與交叉驗證；醫療機構是否建立追蹤、審核與決策紀錄機制。若上述條件皆符合，AI誤判可被視為「可接受醫療不確定性」，醫師與開發商責任得以明確區分。反之，若AI被包裝為高度準確之判讀工具，卻未揭露其對特定病理型態之辨識侷限，則開發商可能涉及資訊揭露不足之產品責任；醫師若未進行必要之交叉檢證，亦可能承擔相應之醫療過失責任。

下，機械手臂於固定脊椎骨釘時發生偏移，致須重新施作，病患遂主張醫療爭議。

2.爭點所在

是否須於手術同意書中揭示AI或手術機器人之使用？純屬機械或系統性偏差時，責任應歸屬於何方？

3.法律評析

在現行法制下，使用手術機器人或即時決策輔助系統，原則上應於手術同意書中揭示其角色、風險與技術限制，否則病患得主張其醫療自主權受侵害。若醫師操作與前置程序皆符合醫療常規，而偏差源於機械或系統缺陷，則涉及醫療過失與產品責任之競合。此時，醫院之設備維護義務與廠商之品質保證責任，將成為責任分流之關鍵，而非當然歸責於執刀醫師。就知情同意義務與醫療自主權上，病患於手術前應充分知悉手術方式、風險及可能替代方案。若手術涉及AI或自動化機器人，醫師應於同意書中揭示其角色、風險及技術限制，否則可能侵犯病患自主權（自決權）。病患應了解醫療程序中所有主要技術或自動化輔助的使用，以保障知情同意。若操作過程符合醫療常規，並無操作疏失，醫師不應承擔全部責任。醫院須確保手術設備維護、檢測及操作流程符合安全標準，如因設備保養不當導致損害，醫院可能承擔管理過失責任。開發商與廠商責任：若偏差源於機械或AI系統設計缺陷、製造瑕疵或警示不足，則可能依《民法》第184條及產品責任原則承擔損害賠償責任。

手術機器人及高風險AI系統為高風險醫療器材，應要求製造商提供明確使用說明與風險揭露，並建立追蹤及監測制度。手術機器人事故中，類型上有「設備瑕疵」與「使用者誤操作」等態樣。AI與自動化手術系統的使用，實際上形成多方參與的醫療決策鏈：醫師（臨床決策）、醫院（流程管理）、廠商（設備及軟體設計）均可能有責任。若無清楚規範，醫師可能因防衛性醫療而過度保守，阻礙AI技術應用。因此，建立明確責任分流框架，是保障病患權益與促進AI技術發展的雙贏之道。

綜合上述案例可知，AI醫療爭議之法律評價核心，並不在於「AI是否正確」，而在於醫師是否已盡合理之專業判斷與注意義務；AI系統之限制是否已充分揭露；醫療機構是否建構適當之管理、監督與風險控管機制。在現行法制下，AI始終定位為輔助工具，最終責任仍歸於人；然隨著技術深化與臨床依賴程度提高，未來責任體系勢將朝向更精緻之多方責任分擔模式發展。

參、資料使用與隱私權法規問題

值此智慧醫療迅速發展之際，人工智慧（AI）之訓練與實際部署，莫不高度仰賴病歷、醫學影像、基因資料及生理音檔等具高度敏感性之個人健康資訊。然近年屢傳醫療機構遭受駭客大規模攻擊，致病人資料遭非法竊取之事件，益發凸顯資訊隱私權於醫療數位化進程中之核心地位與高度爭議性，亦使相關法律風險與責任歸屬問題浮現於檯面

之上[14]，成為不可迴避之重大課題[15]。是以，如何在促進醫療科技創新與智慧應用之同時，嚴格遵循《個人資料保護法》（以下簡稱個資法）及相關醫療法規之規範，實為醫療機構與AI技術開發者所必須共同面對之核心法遵問題。

一、醫囑開立與決策主體：AI代理人之違法風險

關於是否得由AI代理人直接開立醫囑，依現行法制觀之，顯具高度違法風險。按《醫師法》之規定，醫囑之開立，屬醫師專屬之醫療行為，須由具合法醫師資格者，基於專業判斷親自為之，並負最終醫療責任。AI並非法律上之權利義務主體，亦不具醫療專業資格，其功能定位僅得作為臨床決策之輔助工具。縱使AI系統能產出具體醫囑建議，仍須經醫師審核、確認並實際下達，始符合法律要件；否則，恐構成違法行醫，並使相關醫師及醫療機構承擔行政責任、民事賠償責任，甚或衍生刑事風險。

二、資料利用之合法性要件：自去識別化至病人同意

以腎臟內科之臨床管理為例，於病患照護過程中，勢必涉及病歷、透析紀錄、基因數據等屬個人健康資訊之蒐集與處理。倘若擬將此等資料經去識別化或假名化後，用於AI模型之訓練，或與國外研究機構進行資料合作，於個資法及相關法規架構下，究須符合何等法律要件，始得合法進行資料之蒐集、利用與跨境傳輸？又AI系統應如何設計，方能妥善保障病人資料之隱私安全？

依現行法制分析，於個資法之規範下，僅有「不可回復之去識別化資料」，其利用限制始得相對寬鬆；倘僅為假名化處理，仍屬個人資料範疇。其合法要件包括：利用目的須具明確性，並符合目的拘束原則；資料使用應遵循最小必要原則；須建置相當之資訊安全防護措施；並應留存資料利用與存取紀錄，以供事後稽核。至於跨境合作，尚須確保資料接收方具備等值之個資保護水準，並透過研究契約或資料使用協議（Data Use Agreement, DUA）明定責任歸屬，且明文禁止重識別行為。

復就AI訓練或臨床部署過程中，涉及病歷、影像與基因資料之使用，於個資法與醫療法規之框架下，是否須再行取得受試者明確同意？實務上宜採取較為審慎之作法。原則上，建議均取得病人之知情同意；惟若資料已完全去識別化，且僅限於院內照護品質改善用途，得例外免再逐一取得同意。然而，若涉及研究用途、成果發表、跨院共享、商業化應用，或使用基因資料者，則多須取得病人之明確同意，或經人體研究倫理審查委員會（IRB）核准。鑑於基因與影像資

註14：黃鈺玲（2022），《人工智慧應用在醫療領域對隱私權的影響──以侵權行為檢視》，博士論文，國立成功大學。
https://www.firstlaw.com/post/ip/can-artificial-intelligence-have-copyright/

註15：Allen, A. (2011). Unpopular privacy: What must we hide? Oxford University Press；Taiwan Gateway to Health Data（n.d.）。〈願景與任務〉，財團法人國家衛生研究院。

料之高度敏感性，其法遵標準自應提高，以避免侵害病人之自主權與隱私權。

再者，倘醫師私下欲使用院內病人資料進行AI模型訓練，縱無研究發表之計畫，是否仍須申請IRB認可？及是否須徵求病人同意？一般而言，若僅屬醫療品質改善（Quality Improvement, QI）、流程優化或行政管理用途，通常得免送IRB審查；然若AI模型尚具實驗性，或其應用可能影響臨床決策、增加病人風險，即便未涉研究發表，仍建議送交IRB審查，以確保程序正當與風險控管。

於此情境下，IRB不僅係研究倫理審查機制，更具風險控管與程序正當性之法律保護功能。整體而言，雖須視資料是否可識別及其利用目的而定，惟實務上仍建議以取得病人同意為原則。完全去識別化且僅限於院內醫療管理用途者，通常不需逐一同意；然若資料具有可回溯性，或涉及研究、跨境傳輸、商業利用或高風險AI應用，依法與實務見解，均應取得病人明確同意，否則恐有違反個資法及醫療倫理之虞。

至於一般病人在初診掛號時所簽署之資料使用同意定型化契約，是否足以作為日後將其資料用於AI模型訓練之合法依據？依現行法制觀之，多數此類同意書僅涵蓋「醫療與行政目的」，通常不足以直接支撐AI訓練或商業使用之合法性。若AI僅用於院內照護品質改善，解釋空間或可稍寬；然若涉及對外利用、跨院共享或商業化，則建議另行取得具體、明確且可供病人選擇之同意，否則恐有違反目的拘束原則之風險。

又如某醫院進行退化性脊椎病變之機器學習（ML）自動偵測系統建置，其試驗階段主要應注意IRB審查；惟若進一步實施於病人端影像判讀，或進行跨院驗證時，則於病人隱私保護與資料應用上，尚須注意病人告知義務、資料最小化原則、模型版本控管及責任歸屬之明確化。跨院驗證涉及資料移轉，尤應簽署資料共享契約，明確規範去識別化程度、禁止重識別行為及責任分擔，否則一旦發生資料外洩，法律責任恐回歸資料提供之醫院承擔。

再者，若醫院採用地端大型語言模型（LLM）進行加護病房病人轉出入預測，縱其建模資料已由第三方去識別化，然於實際應用病人即時資料時，除健保資料運用授權及病人參與同意書外，尚須注意資訊安全管理制度（ISMS）、資料處理委外契約、模型風險說明文件及資安事件通報機制。即便屬地端部署，凡涉及即時病人資料之處理，仍屬個資處理行為，須符合目的拘束與最小必要原則。

至於將病人影像資料上傳至雲端進行分析之商業AI軟體，其合法性則須視資料是否去識別化、雲端是否位於境外，以及廠商是否提供等值保護而定。依個資法規定，境外傳輸須進行風險評估並留存紀錄。醫院採取「資料不離院」策略，雖屬高度保守，然實為合理之風險控管措施，有助於降低法律與資安責任。

此外，若AI軟體之訓練資料庫非屬公開來源，且隱含偏見，致實際應用後產生系統性誤判，亦可能衍生法律責任。倘因訓練資料偏差，導致特定族群遭受不利判斷，可能構成醫療過失或產品責任問題。AI開發商負有揭露模型限制之義務，醫療機構亦應進行在

地驗證與適用性評估，否則相關風險恐由使用端承擔。

若AI訓練需大量病患資料，於法制上，應優先使用不可回復之去識別化資料，並明確界定利用目的與保存期間；若須使用可回溯資料，則應取得病人同意或IRB核准。基因與透析資料具高度敏感性，更應提高資安與存取控管標準，以避免違反個資法。資料格式之定義亦應兼顧透明性、可執行性與可追溯性，並與國際規範相容，考量不同醫療場域之需求，建立稽核機制，定期檢查資料是否符合標準，並可追溯錯誤來源[16]。

復就AI軟體若具診斷、治療、預測或影響醫療決策之功能，原則上屬醫療器材軟體（Software as a Medical Device, SaMD），須經TFDA審查核准後，方得臨床使用；僅作行政分析或非醫療決策輔助者，始可能免除上市許可。至於AI資安漏洞及病人資料外洩之法律責任，醫院對病人資料負有管理與安全維護責任，防護不足致外洩者，可能違反個資法並負賠償責任；AI廠商則依契約關係與侵權法理負責。是以，資安條款、事故通報及責任分配機制，實不可或缺。

就病患資料與隱私保護而言，當AI訓練需大量醫療數據時，如何在符合個資法或《GDPR》之前提下合法使用？於匿名化與可回溯性間，法律上雖傾向不可回溯以降低風險，然醫療實務仍有追蹤需求。是以，建議採行「分離式假名化」及權限控管，由獨立單位掌握解碼權限，僅於必要時回溯，以兼顧研究、照護與隱私保護。

肆、結論

面對未來AI具備自主學習能力，甚至可能產生設計者亦難以預測之行為時，傳統法律所倚賴之「可預期風險」判準，勢將遭受重大衝擊。尤以介入性放射科等高度仰賴影像決策之醫療領域為甚，現行法制對於AI介入治療路徑之權責劃分、決策過程之審查與紀錄標準，仍顯不足，亟待補充。

至於醫師如何適法使用AI，醫事人員宜遵循以下原則：（一）檢證義務：將AI視為「第二意見」，不得盲從，並保持獨立之專業判斷；（二）記載與說明：當臨床決策與AI建議不一致時，應於病歷中詳實記載其理由；（三）充分告知：對於AI參與決策之風險與限制，應對病患履行告知義務；（四）遵循常規：確保AI之使用符合既有醫療指引，並持續監控其於個別病患之適用性。

醫療機構於臨床輔助中使用AI時，尤應將「目的拘束」與「最小必要原則」奉為最高指導原則。無論係地端部署之大型語言模型，抑或影像判讀工具，除基本之病人同意與IRB核准外，尚須完善模型風險說明文件與資料處理委外契約。此外，醫療人員之臨床操作行為監測，亦屬隱私權保護之範疇，應於管理規範中一併制度化處理，以確保智慧醫療之發展，得在法治與倫理之軌道上穩健前行。

註16：黃詩淳（2023），〈AI可解釋性的法學意義及其實踐〉，《台大法學論叢》，52(S)，第931頁。https://doi.org/10.6199/NTULJ.202311/SP_52.0001