

立法院法制局專題研究報告

編號：1866

本報告僅供委員參考

人工智慧應用於醫療領域法制問題研究

法制局 黃嘉文 撰

中華民國 115 年 9 月

人工智慧應用於醫療領域法制問題研究

目 次

摘要

壹、前言.....	1
貳、AI 應用於醫療領域概況.....	2
參、AI 應用於醫療領域之國際立法趨勢.....	5
一、世界衛生組織.....	6
二、歐盟.....	9
三、美國.....	13
肆、我國 AI 應用於醫療領域之相關規範.....	18
一、醫療器材管理相關法規.....	18
二、負責任 AI 執行中心.....	20
三、醫療機構應用生成式人工智慧指引.....	21
伍、問題研析與建議.....	23
一、建立完整的 AI 醫療風險分級及管理規範.....	23
二、明確 AI 醫療之責任歸屬，並研議救濟、補償或保險機制.....	25
三、強化 AI 醫療隱私保護規範.....	27
四、研議訂定 AI 應用於心理健康領域之管理規範.....	29
陸、結論.....	32
參考文獻.....	33
附錄：「人工智慧應用於醫療領域法制問題研究」專題研究報告（初稿） ）座談會紀錄及參採情形.....	39

摘 要

人工智慧（Artificial Intelligence）在醫療領域上已產生革命性的影響，包括臨床決策支援和輔助系統、疾病診斷、藥物開發以及個人化醫療等多方面，為醫療體系的運作帶來效率提升和精準化服務。儘管其潛力巨大，AI在醫療中的實際應用仍存在許多挑戰，如資安風險與倫理治理問題正同步攀升。目前國際上對於AI在醫療領域上的管理，都以不同的法律規範來因應，我國亦不例外。本報告爰簡介前開法律規範，研析相關法制問題並提出建議，俾供本院委員問政參考。

人工智慧應用於醫療領域法制問題研究

壹、前言

人工智慧 (Artificial Intelligence, 下稱 AI) 是一個多技術結合的領域，尤其是近年大型語言模型所開發之生成式 AI (Generative AI) 問世後，透過機器學習和深度學習，可以生成新的數據或內容，包括圖像、音訊、文本和影像。這些技術都能改變醫療、創意、產業和科學研究的面貌，每種方法也都有其特定的生成機制和應用場景，尤其在醫療應用中更展現出不同以往的發展潛力，顯著提升效率和精準度¹。

隨著 AI、大數據與雲端技術快速融入醫療體系，智慧醫療正重塑診療模式與醫療服務流程。從影像判讀、臨床決策支援，到遠距醫療與疾病風險預測，儘管 AI 在醫療領域的應用帶來了許多好處，但其缺點和挑戰同樣不容忽視。首先，AI 系統的可靠性問題是當前最大的挑戰之一，儘管 AI 能夠分析大量數據，但它並不具備人類醫生的臨床經驗和直覺，這意味著在某些情況下，AI 的診斷可能會出現錯誤，導致誤診或漏診。因此，醫療行業依然需要依賴專業醫生的判斷來驗證 AI 的診斷結果。其次，AI 系統的設計和訓練需要大量高品質的數據。然而，醫療數據的獲取和處理並不容易，尤其是在涉及個人隱私的情況下。數據的品質、數量、完整性和來源都會直接影響 AI 系統的準確性。如果數據存在偏差或不準確，那麼 AI 系統的運作效果也會受到影響，進而可能導致不良的醫療結果。另外，AI 系統的透明性和可解釋性問題也引起了廣泛的關注。許多 AI 模型在做出

¹ 黃維民，〈從醫管專業的觀點探討生成式醫療人工智慧的倫理與規範〉，《電腦稽核》，第 53 期，115 年 2 月，頁 4。

決策時，過程往往被視為「黑盒子」(Black Box)，這使得醫生和患者難以理解其背後的邏輯。缺乏可解釋性不僅使得醫療專業人員難以信任 AI 的診斷，還可能令患者在面對治療選擇時感到困惑。這些挑戰使得在醫療領域全面推廣 AI 的過程變得複雜而艱難²。

隨著人口高齡化、慢性病負擔加重，以及科技進步，AI 技術正深刻改造醫療服務。AI 已逐步成為提升醫療效率與品質的重要工具，但在這場技術革新的背後，卻也衍生出一些問題，如資安風險與倫理治理問題正同步攀升，甚至呈現結構性放大，成為影響醫療體系安全與信任的核心挑戰。醫療體系的根本是建立於「信任」之上，而信任的基礎，正是對資訊安全與專業治理的依賴。醫療機構所持有的資料，具有高度敏感性與隱私性，一旦外洩不僅僅是侵犯隱私，更可能引發社會排除等長期後果。相較於其他產業，醫療資料的風險並非短期財務損失，而是長期且難以回復的個人與社會損害³。

本報告擬簡介外國及我國對於 AI 應用於醫療領域目前相關法規治理的情形，研析相關法制問題並提出建議，俾供本院委員問政參考。

貳、AI 應用於醫療領域概況

AI 是現今「智慧醫療」(eHealth) 的核心技術之一⁴，AI 技術透過機器學習 (Machine Learning，下稱 ML)、資料探勘 (Data mining)

² ReBlood，AI 醫療真的都是優點嗎？AI 醫療缺點及挑戰大曝光，113 年 11 月 21 日，網址：<https://rebloodgroup.com/ai-pros-cons/>，最後瀏覽日期：115 年 7 月 31 日。

³ 周迺寬，〈醫療人工智慧時代下的資安風險、倫理治理與制度建構—從臺灣近年醫療資安事件談「負責任 AI」的關鍵基石〉，《消費者報導雜誌》，第 542 期，115 年 6 月，頁 27。

⁴ 陳芳毓，智慧醫療懶人包》八張圖，一次搞懂智慧醫療的定義、應用與台灣的挑戰，天下雜誌，112 年 1 月 1 日，網址：<https://futurecity.cw.com.tw/article/1916>，最後瀏覽日期：115 年 7 月 31 日。

等演算程式，將數據資料潛在價值發揮最大化，如此全面性的技術變革，促進智慧醫療及精準醫療等前瞻性的醫學進步⁵。根據統計，2024⁶年全球 AI 在醫療健康照護市場規模達到 323.4 億美元，預計到 2032 年將快速成長到 4,310.5 億美元，年複合成長率高達 38.23%，而 AI 醫療技術發展，正從單一任務工具進化為全病程管理與臨床決策支援平台⁷。目前 AI 在醫療領域的運用內容如下⁸：

一、醫療診斷與監測

AI 輔助診斷是目前最受矚目的研發方向，無論是以數值為主體的檢體化驗與生命徵象，或是以波形特徵進行判斷的心電圖，甚至是以圖像異常變化為依據的各類醫療影像（如：電腦斷層 CT、核磁共振 MRI、超音波、眼科影像與病理切片等），均有高效且準確的 AI 輔助診斷系統案例被成功研發。除了單一項目的輔助診斷外，許多機構也開發出可彙整病患綜合資訊並進行自動化警告的監測系統，以全天候協助醫護人員確保病患安全，讓醫療團隊能及早介入急重症病患，避免疾病惡化與危及生命。

二、遠距與居家醫療

AI 也讓醫療超越時間與空間的限制，提供遠距醫療的機會。透

⁵ 蕭佳敏，〈運用人工智慧技術於醫療的法律風險與隱憂－利弊互現〉，《靜宜法學》，第 13 期，113 年 12 月，頁 64。

⁶ 本報告有關年分之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。

⁷ 李永健，全球 AI 醫療照護與器材發展趨勢探討，IEK 產業情報網，114 年 6 月 12 日，網址：https://ieknet.iek.org.tw/iekrpt/rpt_more.aspx?rpt_idno=643636041，最後瀏覽日期：115 年 7 月 31 日。

⁸ 曾柏諺，人工智慧在醫療領域的應用與挑戰－資訊科技在生醫領域擦出新火花，中國醫藥大學學生會，115 年 7 月 20 日，網址：<https://www.twcmusa.org/column/%E4%BA%BA%E5%B7%A5%E6%99%BA%E6%85%A7%E5%9C%A8%E9%86%AB%E7%99%82%E9%A0%98%E5%9F%9F%E7%9A%84%E6%87%89%E7%94%A8%E8%88%87%E6%8C%91%E6%88%B0%EF%BC%8D%E8%B3%87%E8%A8%8A%E7%A7%91%E6%8A%80%E5%9C%A8%E7%94%9F/>，最後瀏覽日期：115 年 7 月 31 日。

過整合智慧型穿戴式裝置、感測器與 5G 高速網路，配合 AI 整合與監測數據，可以讓醫療團隊運籌帷幄之中，決勝千里之外，協助偏遠地區民眾進行診療或實現居家醫療服務。同時，生成式 AI 模型（如 GPT4.0 等）也能協助患者就醫相關事項與衛教宣導，滿足遠距及居家患者及時的需求。

三、醫療工具開發

AI 也促進新一代醫用工具與治療手段的開發與研究，如目前外科領域新興的達文西手術機器人即在操控輔助、實時影像處理、手術自動化與手術影像輔助等模組研擬加入 AI 系統，使手術進行更便捷、高效與精準。除了外科領域外，AI 的加入也讓藥物研發與試驗方法有突破性發展，透過 AI 在反應模擬與預測效能的能力，可以大幅縮短藥物開發週期並降低研發成本，並創造更多治療的可能性。

四、醫療管理、行政與研究

在醫院管理方面，AI 可以分析病患與營運資料，預測人力、耗材與床位需求，以增進醫院營運效率與降低成本和碳排放。在醫療行政上，透過自然語言處理工具與生成式 AI 模型，也可以在病歷繕打與癌症登記等文書工作上提升效率與降低人為錯誤。同時 AI 的大量數據解析與預測能力，也協助醫學與流行病學研究，藉此實現精準醫學與早期風險評估並提升醫療品質的效果。

此外，生成式 AI 巨大的潛力，也應用在醫療保健的多個領域。在製藥產業方面，生成式 AI 可用於藥物開發、生產製造、物流與供應鏈管理、以及銷售與客戶服務等階段。藥物開發方面，它能分析文獻與數據以發現新候選藥物，優化臨床試驗設計，加速研發進程；在生產製造方面，生成式 AI 能夠優化生產流程、監控品質、預測供應

鏈情況，提高生產效率；在醫療器材產業，生成式 AI 亦可應用於研發和銷售服務。在研發方面，它能加速軟體開發流程，自動生成文件與紀錄，提高設計效率；在銷售服務方面，它能分析市場資訊，提升服務品質，簡化產品說明，改善使用者體驗；在臨床場域方面，生成式 AI 則可應用於醫療現場及醫院管理等方面。而 AI 也能自動生成病歷文件、協助病情判斷、優化醫院管理流程，為臨床醫師提供治療建議，提升服務品質⁹。

綜上，AI 對於現今智慧醫療的助益，已顯現在許多的面向上，改變了傳統醫療的效率及品質，包括¹⁰：

- 一、協助醫療決策：發展醫院的數位決策管控中心，整理資料分析，有助於加速醫院處理急症的效率。
- 二、增進醫病關係：導入數位科技與 AI，協助改善流程，並增進患者體驗與醫病關係。
- 三、簡化行政流程：透過流程機器人和人工智慧等技術，讓照護者專注在照護工作，而非將時間耗費在行政工作。
- 四、優化服務流程：分析醫院服務瓶頸，透過醫院服務流程設計優化，提升服務品質。
- 五、提升營運效率：導入數位供應鏈、自動化及機器人等技術，提升營運管理和後台效率。

參、AI 應用於醫療領域之國際立法趨勢

AI 雖已廣泛應用於各項醫療領域，但也衍生相關的問題，包括醫

⁹ 吳振吉，AI 革命下的醫療新紀元：應用潛力與法律挑戰，天下雜誌，113 年 4 月 25 日，網址：<https://futurecity.cw.com.tw/article/3399>，最後瀏覽日期：115 年 7 月 31 日。

¹⁰ 工研院產業學院，AI 智慧醫療是什麼？一篇文帶你了解台灣智慧醫療的現況，工研院產業學習網，111 年 7 月 11 日，網址：<https://college.itri.org.tw/Info/InfoData/1d549534-07c6-4407-b1de-d5a04ddd665c>，最後瀏覽日期：115 年 7 月 31 日。

療責任的歸屬、資料使用的隱私權、資訊安全隱憂、偏見與歧視、準確性與黑天鵝式幻覺現象 (hallucinations)、醫療器材監管、智慧財產權、產品責任、過度依賴與倫理規範等¹¹。為因應使用AI所可能產生的問題，國際上有許多相關管理規範，簡述如下：

一、世界衛生組織

世界衛生組織 (World Health Organization, 下稱WHO) 於2021年發布「AI運用於健康領域的倫理與治理指引」(Ethics and governance of artificial intelligence for health)，這是WHO諮詢多位AI領域頂尖專家後，指出在醫療保健中使用AI的潛在好處和風險，並提出6項達成共識的原則，提供政府、研究者與醫療提供者在使用AI時的參考，這些原則包括¹²：

- (一) 保護人類的自主權 (Protect autonomy)：認為人類仍應掌有關於醫療保健系統全部之決定權，而AI只是輔助功能，無論是醫療服務提供者或病人，皆應在知情之狀態下作決定或同意。
- (二) 促進人類福祉、安全、公共利益(Promote human well-being, human safety and the public interest)：AI不應該傷害人類，因此須滿足事前相關監管要求，同時確保其安全性、準確性及有效性，且其不會對病人或特定群體造成不利影響。
- (三) 確保透明度、可解釋性與可理解性 (Ensure transparency, explainability and intelligibility)：開發人員、用戶、及監管機構應理解AI所作出之決定，故須透過記錄與資訊揭露

¹¹ 黃維民，同註1，頁13-14

¹² WHO, Ethics and governance of artificial intelligence for health, Jun. 28, 2021, available at : <https://www.who.int/publications/i/item/9789240029200>, last visited on Jul. 31, 2026.

以提高其透明度。

(四) 培養有責性和歸責制度 (Foster responsibility and accountability)：AI在醫學中所涉及之內部責任歸屬相當複雜，關於製造商、臨床醫師及病患間問責機制之設計，將會成為各國之挑戰，故須存在有效的機制來確保問責性，也應避免責任分散之問題產生。

(五) 確保包容性和公平性 (Ensure inclusiveness and equity)：應鼓勵應用於健康領域之AI能被廣泛且適當地使用，無論年齡、性別、收入及其他特徵而有差別待遇，且應避免偏見之產生。

(六) 促進回應迅速且可持續性的AI (Promote artificial intelligence that is responsive and sustainable)：人工智慧應符合設計者、開發者及用戶之需求與期待，且能充分具適應性之回應且符合使用環境中之要求。

WHO於2024年1月再次更新本指引，探討了大型多模態模型 (Large Multimodal Models, LMMs) 可能的影響，並發布新的指引 (Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models)，該指引概述了 40 多項建議供政府、科技公司和醫療保健提供者參考，以確保合理使用 LMMs 來促進和保護人群健康¹³。LMMs用途廣泛，可協助許多醫療領域事項，執行重複性的臨床行政工作，醫事人員可更專注在臨床職責，解決複雜度高的問題與決策。但WHO認為，LMMs可能有相關的問題與風險，

¹³ WHO, Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models, Mar. 25, 2025, available at : <https://www.who.int/publications/i/item/9789240084759>, last visited on Jul. 31, 2026.

包括：(一) 高估LMMs的效益並低估風險；(二) 可及性和可負擔性；(三) 系統上的偏差；(四) 對勞動市場的影響；(五) 不合宜的LMMs；(六) 網路安全風險¹⁴。為避免上述問題與風險，WHO提出針對LMMs的AI價值鏈關鍵3階段，應採取適當的治理，包括(一) 開發者(developer，如開發LMMs的科技公司)應導入實際規範，來確保AI工具的設計和開發過程符合倫理與法規，避免誤診等情形，並遵守醫療倫理準則；(二) 提供者(provider，如引進使用LMMs的醫院)應評估和監管醫療領域使用LMMs的情況，確保應用者接受適當的培訓，並保護病人隱私；(三) 應用者(deployer，如使用LMMs的一線醫護人員)：遵循正確的操作流程，並及時判斷、處理LMMs任何可能的錯誤或疏漏。此外，政府亦可透過制定法律政策、監管AI使用以及提供相關培訓課程等方式，監管LMMs在醫療領域的使用¹⁵。

WHO另於2025年11月19日發布「人工智慧正在重塑醫療系統：世衛組織歐洲地區準備情況報告」(Artificial intelligence is reshaping health systems: state of readiness across the WHO European Region)，該報告為2024年至2025年於WHO歐洲地區醫療照護領域人工智慧(AI for health care)調查結果，借鑑50個成員國之經驗，檢視各國之國家戰略、治理模式、法律與倫理框架、勞動力準備、資料治理、利益相關者參與、私部門角色以及AI應用之普及情況，探討各國如何應對AI於醫療系統中之機會與挑戰。其中責任規則(liability rules)之建立，為成員國認為推動AI於醫療照護領域廣泛應用之最重要關鍵政策因素，因此該報告建議應明確開發者、臨床醫生、資料提供者與醫療機構之責任，透過救濟與執法管道以保護

¹⁴ 蕭佳敏，同註5，頁81-82。

¹⁵ 戴于揚、陳哲民、吳逸帆、吳欣潔、郭冠良，〈論2024年WHO發表之「人工智慧於健康領域之倫理與治理」與台灣現況〉，《台灣家庭醫學雜誌》，第34卷，第3期，113年9月，頁139-140。

病患與醫療系統之權益¹⁶。

二、歐盟

歐盟致力於推動一個集中及橫向的立法計畫，使責任制度現代化。然而，2025年此一具指標性策略出現重大轉折，即《AI責任指令》（AI Liability Directive）因分歧過大而暫時撤回。目前歐盟的監理版圖包含3項與醫療AI相關的主要法規工具：

（一）醫療器材法規與軟體醫療器材

歐盟第2017/745號法規（EU Medical Device Regulation，下稱MDR）規範管轄關於歐盟市場使用的醫療器材—包括符合醫療器材定義的軟體（Software as a Medical Device，下稱SaMD），亦即用於診斷、預防、監控或治療的軟體被視為器材，並依風險分類。另MDR建立了分類規則、符合性評鑑程序及上市後監督義務（上市後監測要求），這些規定適用於符合器材定義的AI賦能軟體。一切器材含軟體均需遵守MDR，且以取得歐洲合格認證標誌為商業部署的主要市場進入要件。再者，MDR強調臨床證據與上市後性能監控，要求SaMD製造商規劃持續臨床評估、風險管理及網路安全措施¹⁷。

（二）修訂版產品責任指令

隨著研議中的《AI責任指令》因政治分歧於2025年2月被撤回，歐盟實際上透過修訂版《產品責任指令》（Product Liability Directive，下稱PLD），將1985年關於瑕疵產品的指令現代化，把嚴格責任概念延伸至數位產品與軟體，並引入推定機制，使受害者

¹⁶ 施雅薰，世界衛生組織發布歐洲區域人工智慧於醫療系統準備情況報告，責任規則為最重要之關鍵政策因素，Stli，115年1月18日，網址：https://stli.iii.org.tw/article-detail.aspx?no=65&tp=1&d=9442#_ftn1，最後瀏覽日期：115年7月31日。

¹⁷ 張冠群，〈醫療人工智慧的責任、監理與責任保險問題：歐盟與美國法制之初探及責任保險制度在設計之芻議〉，《全國律師》，第30卷，第1期，115年1月，頁59-60。

在技術複雜的案件中更容易證明因果關係。新版PLD擴大了「產品」的定義以納入AI與軟體，亦即透過明確定義軟體和AI系統為「產品」，解決數十年的不確定性。這使得開發者需對漏洞、演算法錯誤和設計缺陷承擔嚴格責任，擴大可請求賠償的損害範圍，延長售後義務，在原告面臨過度技術困難時創設瑕疵與因果關係之推定，並強化嚴格責任（Strict Liability）這些變革為軟體製造商與數位產品供應商帶來巨大的潛在法律風險。另傳統上的「開發風險抗辯」（Development Risk Defense）允許製造商在證明流通時科學知識水平無法發現缺陷的情況下免責，而修訂版PLD針對AI大幅限縮此項抗辯。如果缺陷是由於缺乏必要的軟體更新，或者製造商保留對軟體的控制權，此項抗辯則不適用。再者，新版PLD採用瑕疵推定制度，其為解決「黑盒子」證據缺口，引入可推翻的推定（Rebuttable Presumptions）制度，若請求權人因技術複雜性而在證明缺陷方面面臨過度困難，且能證明該產品「可能」造成損害，法院可推定該產品存在缺陷，此有效地將舉證責任轉移至製造商，要求其證明AI沒有缺陷，這對病患而言是一個巨大的程序優勢¹⁸。

（三）人工智慧法

歐盟《人工智慧法》（Artificial Intelligence Act，下稱AIA）自2024年8月1日正式生效，並建立風險導向監管架構（Risk-Based Approach），將AI用途之風險程度分為4種監理等級，而高風險（High Risk）等級係指在健康、安全、基本權利等重要領域具有重大影響力的AI系統，其中就包含醫療診斷、問診、治療輔助、醫療器材¹⁹。使

¹⁸ 同前註，頁 60-61。

¹⁹ European Commission, AI Act, Aug. 1, 2025, available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai?> last visited on Jul. 31, 2026.

用高風險AI系統時，宜啟用「人為監控」其運行，包括檢測和解決異常，以防發生侵害健康、安全或基本權利風險。同時應維持AI系統準確性、穩健性和網路安全，並建立品質管理體系。高風險AI系統運行過程亦應留下日誌紀錄，並有除錯機制，適時修正程式。AIA對於系統提供者、進口商、經銷商、應用者分別定有相對義務，而政府機關應建置至少一個AI的「監管沙盒」(Regulatory Sandbox)，用於AI技術開發、訓練和測試²⁰。AIA在透明度、資料治理、技術穩健性、真人監督及文件記錄方面皆訂定使用者義務；因此，它與MDR的義務直接交集，呈現競合關係，亦即符合醫療器材資格的AI系統需同時滿足兩套法律的規範要求，形成疊加合規義務，並對醫療AI的製造商與使用者施加新的法令遵循義務。法條強制規定高風險AI系統的設計必須能實現有效的真人監督(human oversight)。此條款對責任至關重要，如果製造商未能設計足夠的監督工具，其即違反了法定安全要求，從而引發責任。反之，若工具存在但醫師未使用，責任則轉移至醫療提供者²¹。

AIA涵蓋醫療領域在內的各個領域之AI技術應用，且其目標為協助歐盟各成員國提供全面、透明與可預見的法規框架，以規範AI技術的開發與使用，並保護公眾的權益與價值觀。該法案中涉及幾項與醫療領域相關的要點：首先，該法案要求醫療AI技術應遵循醫療倫理原則與隱私權保護原則；其次，AI技術於醫療領域中的使用應符合安全性、可靠性與隱私權保護等要求；此外，醫療AI技術須經過充分的測試與驗證，以確保其符合醫療倫理與法律法規的要求；最後，該法案明確禁止使用AI技術替代專業醫師或醫護人員而做出重大的醫療

²⁰ 蕭佳敏，同註5，頁85-86。

²¹ 張冠群，同註17，頁60。

決策，同時強調AI技術開發與使用的透明度與責任追究原則²²。

AIA生效後，與MDR及《體外診斷醫療器材法》(In Vitro Diagnostic Medical Devices Regulation，下稱IVDR)高度重疊，特別是針對用於醫療目的之人工智慧系統(Medical Device AI，下稱MDAI)。為釐清三法協同適用原則，歐盟人工智慧委員會(Artificial Intelligence Board, AIB)與醫療器材協調小組(Medical Device Coordination Group, MDCG)於2025年6月19日聯合發布常見問答集指引(Frequently Asked Question, FAQ)，系統性說明合規原則與實務操作方式，涵蓋MDAI分類、管理系統、資料治理、技術文件、透明度與人為監督、臨床與性能驗證、合規評鑑、變更管理、上市後監測、資安與人員訓練等面向。過去，MDR、IVDR與AIA雖各自對MDAI有所規範，但始終缺乏明確的協同適用指引，導致製造商、監管機關與醫療機構在實務操作上常面臨混淆與困難，而該指引透過36題問答，系統性釐清三法在高風險MDAI適用上的關聯，重點涵蓋產品分類原則、合規評鑑流程以及技術文件準備要點，具高度實務參考價值。此外，傳統醫療器材的上市後監測，難以有效因應AI系統持續學習所帶來的風險。AIA因此要求高風險MDAI建立強化的上市後監控系統，並評估AI系統與其他系統交互作用可能產生的影響。整體而言，該指引的發布不再僅限於MDAI技術層面的合規審查，而是進一步擴展至資料正當性、系統可控性、使用者能力與整體風險治理等層面，體現歐盟對AI倫理、透明與責任的制度化落實。此文件亦為歐盟首次系統性整合AI與醫療器材監管原則，預期將成為MDAI產品研

²² 苗光磊，〈人工智慧技術應用於醫療領域所衍生之隱私權保護的法律規制〉，《全球知識發展期刊》，第2卷，第4期，113年12月，頁7。

發與上市的重要參考依據²³。

三、美國

與歐盟的集中式改革形成鮮明對比，美國並未訂有 AI 相關管理專法，而是透過聯邦法規與州普通法（Common Law）組成的架構來管理醫療 AI 責任：

（一）人工智慧醫療器材監管

美國食品藥物管理署（Food and Drug Administration，下稱 FDA）負責醫療器材軟體的監管。器材的分類決定了製造商享有的責任與保護²⁴。隨著 AI 在醫療器材的應用日益增加，美國 FDA 自 2019 年以來便不斷增訂修正相關監管方法。其中最重要的開端始於 2019 年 4 月，當時美國 FDA 向業界發布「使用人工智慧/機器學習演算法醫療器材軟體變更之管理框架」（Proposed Regulatory Framework for Modifications to Artificial Intelligence / Machine Learning 【AI/ML】-Based Software as a Medical Device 【SaMD】），作為監管架構初步的提案以及徵求利害關係人的回饋。在這份文件中，美國 FDA 針對多個主題徵求意見，包括人工智慧/機器學習（Artificial Intelligence/Machine Learning，下稱 AI/ML）醫療器材上市前審查、上市後修改的監管評估，以及評估品質的方法。美國 FDA 於 2021 年 1 月回應大量利害關係人的回饋，發布「基於人工智慧/機器學習技術之醫療器材軟體行動計畫」（Artificial Intelligence/Machine Learning 【AI/ML】-Based Software as a Medical Device 【SaMD】 Action Plan）。在此行動計畫中，美國

²³ 呂政諺，歐盟發布人工智慧法、醫療器材法與體外診斷醫療器材法協同適用問答集，Stli，114 年 7 月，網址：<https://stli.iii.org.tw/article-detail.aspx?tp=1&d=9376&no=64>，最後瀏覽日期：115 年 7 月 31 日。

²⁴ 張冠群，同註 17，頁 61。

FDA 承諾採取五大特點來持續監管應用 AI 的醫療器材²⁵：

- 1、為應用AI的醫療器材量身訂製監管框架：美國FDA認知到需要制定特殊的指導方針以支持AI/ML醫療器材的發展，並承諾推廣這些指導方針，尤其是在上市後變更控制方面。
- 2、良好機器學習實踐（Good Machine Learning Practice，下稱GMLP）原則：美國FDA將與國際監管社群合作制定GMLP原則，用以指導產品開發和維護。
- 3、以患者為中心、融入對使用者的資訊透明度：美國FDA將致力於傳播AI/ML醫療器材的相關資訊，包括用於演算法訓練的資料來源，以及確保所有使用者都能輕鬆了解AI/ML醫療器材的益處、風險和限制。
- 4、與演算法偏見相關的監管方法：美國FDA承認，雖然偏見並非AI/ML醫療器材所獨有，但大眾會對這些設備及其功能所依據的資料相關的偏見持有特別的擔憂。美國FDA承諾支持關於監管的科學研究，以確保在AI/ML醫療器材的開發和維護中考慮及於諸如種族、民族和社會經濟地位等因素。
- 5、整合實際性能指標：美國FDA認為真實世界數據（real-world data）在AI/ML醫療器材的開發和監管中會是非常重要的議題。AI/ML醫療器材的普遍性，也就是在和模型訓練資料不同的環境、病人下，性能是否能維持將是一大重點。美國FDA承諾將徵求一些廠商自願提供真實世界數據來試行監測，以此來訂定適用於AI/ML醫療器材監管的實際性能指標。

²⁵ FDA, Artificial Intelligence in Software as a Medical Device, available at: <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-software-medical-device>, last visited on Jul. 31, 2026.

自宣布 2021 年行動計畫以來，美國 FDA 持續發布多份指導文件，以履行其對 AI/ML 醫療器材之監管相關的承諾。2021 年 10 月，定義何謂良好機器學習實踐的 10 項準則（Good Machine Learning Practice for Medical Device Development: Guiding Principles）率先被發表。2022 年 9 月，美國 FDA 在「臨床決策支援軟體指引文件」（Guidance document on Clinical Decision Support Software）更加清楚地定義哪些輔助臨床決策的軟體屬於醫療器材並將受到規範，其中部分軟體包括預測敗血病、預測心臟衰竭病患住院機率，並將鑑別可能成癮於鴉片類藥物病人的演算法納為醫療器材規範。隨後在 2023 年發表的兩份草案「針對人工智慧與機器學習醫療器材軟體所發布的預定變更控制計畫上市提交建議指引」（Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning **【AI/ML】**-Enabled Device Software Functions）及「機器學習啟用醫療器材預定變更控制計畫指導原則」（Predetermined Change Control Plans for Machine Learning-Enabled Medical Devices: Guiding Principles）皆針對 AI/ML 醫療器材廠商在申請上市前需繳交的預定變更控制計畫（Predetermined Change Control Plan，下稱 PCCP）提出更詳細的建議。廠商需提供詳細的變更計畫、清楚解釋器材變更之應用及驗證方法學、以及變更後可能造成的影響評估。美國 FDA 也在草案中指出，廠商必須敘明日後如何向用戶溝通器材變更的必要資訊。2024 年 3 月，美國 FDA 再次發布「生物製品評估與研究中心、藥品評估與研究中心、器材與放射健康中心和複合產品辦公室等部門在人工智慧醫療產品上如何共同合作」（Artificial Intelligence and Medical Products: How CBER, CDER, CDRH, and OCP are Working Together），

主要作為補充 2021 年發布的行動計畫，並強調各部會之間的合作規劃²⁶。

（二）AI 治理指引

全美各州醫療委員會聯合會（The Federation of State Medical Boards，下稱 FSMB）於 2024 年 4 月發布「引導人工智慧以負責任與符合倫理方式融入臨床實務」（Navigating the Responsible and Ethical Incorporation of Artificial Intelligence into Clinical Practice）指引，明確概述醫師於利用 AI 協助提供照護時可採取之步驟，以履行其倫理與專業職責，期能藉此降低對患者造成傷害之風險；本指引之特色在於，其要求醫師為 AI 之利用結果負最終之責任。FSMB 向各州醫療委員會與其他利害關係人所提供之原則與建議如下，以支持對包含 AI 之臨床照護進行負責任與符合倫理之監管²⁷：

1、透明度與揭露（Transparency and Disclosure）：應要求維持於醫療照護領域使用 AI 之透明度；各州醫療委員會應制定明確之指導方針，向患者揭露 AI 之使用情況，其有助於患者與醫師之理解，但不會造成不必要之行政負擔；FSMB 應制定文件，詳細說明最常用之 AI 工具之功能與局限性，以協助醫療委員會發揮監管者之角色，並應制定常見問題與最佳實務文件，作為提供照護時利用 AI 方面關於透明度之資源。

2、教育與理解（Education and Understanding）：FSMB 及其於醫學教育界之合作夥伴，應為醫師、醫療委員會與患者，確認有關醫

²⁶ 陳昱安，人工智慧醫療器材該如何監管？以美國經驗為例，DSET，113 年 4 月 19 日，網址：<https://dset.tw/research/00010/>，最後瀏覽日期：115 年 7 月 31 日。

²⁷ 施雅薰，全美各州醫療委員會聯合會發布人工智慧（AI）治理指引，並要求醫師為 AI 之利用結果負最終責任，Stli，113 年 9 月，網址：<https://stli.iii.org.tw/article-detail.aspx?tp=1&d=9239&no=64>，最後瀏覽日期：115 年 7 月 31 日。

療照護中AI之結構化教育資源，該等資源應包括協助瞭解AI如何運作、其優點、潛在風險以及對患者照護之影響。

- 3、負責任之使用與問責 (Responsible Use and Accountability)：開發人員應協助醫師瞭解何時、以及如何於患者之照護中利用AI工具；選擇AI工具支援臨床決策之醫院系統、保險公司或其他機構應向醫師提供有關AI工具之教育、存取各工具之性能報告，並應設計一個定期檢視工具功效的流程；AI工具應以得使各州醫療委員會能稽核與理解之方式設計，以便適當評估依賴工具輸出結果之醫師是否偏離照護標準 (standard of care)；FSMB應支持各州醫療委員會針對臨床醫師如何負責任、可問責地使用AI之解釋。
- 4、公平性與近用 (Equity and Access)：應努力確保所有患者皆能公平地近用AI帶來之好處；FSMB與各州醫療委員會致力於以下原則：醫療人員所提供之照護是公平的、且不受基於種族、民族或其他形式歧視之偏見影響；FSMB應與其他利害關係人一起理解並解決演算法偏差問題。
- 5、隱私與資料安全 (Privacy and Data Security)：AI工具之開發者必須實施嚴格之保護措施，以保護AI開發與評估時所利用之患者資料，通常情況下應告知患者資料如何被利用，且FSMB應與行業利害相關人一起制定AI系統使用與散布患者資料之政策，包括針對AI開發或評估中使用之患者資料之最低資料保護措施。
- 6、監督與監管 (Oversight and Regulation)：各州醫療委員會必須保留對於提供醫療服務時，不當應用AI工具之醫生進行紀律處分之權力，特別是當AI系統變得更加自主時；另各州醫療委員會應審查其管轄範圍內如何對「醫療行為」(practice of medicine) 進行法律定義，以確保對提供醫療照護、人力或其他方面進行持

續之監管監督。

7、法令之持續檢視與調整 (Continual Review and Adaptation of Law and Regulations)：各州醫療委員會應在FSMB之支持下，隨著AI不斷發展，持續檢視與更新與AI相關之指引與法規；政策制定者應考慮AI對基本法律原則的影響，例如醫療行為之定義以及AI對企業醫學實務之影響；FSMB應建立一個專門團隊，持續檢視與調整AI指引與法規。本指引指出，AI工具通常無能力取代醫師之專業判斷、倫理責任或對州醫療委員會之責任，醫療行為中之關鍵職業責任始終為確保診斷、臨床決策與建議不存在偏差。與用於診斷或治療疾病之任何其他工具或鑑別方法相同，醫療專業人員有責任確保基於證據結論之準確性與真實性，因此於將AI系統用於患者照護前，醫師應以合理努力識別與解決偏差。

肆、我國 AI 應用於醫療領域之相關規範

為大力發展智慧醫療產業及將智慧醫療軟體導入於臨床治療、健康照護、公共衛生及醫學研究等領域，我國關於 AI 應用於醫療領域之現行法制概況如下：

一、醫療器材管理相關法規

我國於 109 年 1 月 15 日公布《醫療器材管理法》，該法第 3 條明定如用於診斷、治療、緩解或直接預防人類疾病之醫療器材軟體（包含醫療器材人工智慧軟體），則應受該法相關規定所管制，以確保醫療器材使用安全、效能及品質²⁸。近年來，衛生福利部（下稱衛福部）也發布多項 AI/ML 技術醫療器材相關的技術指引，以期協助業者順

²⁸ 吳英志，〈從負責任 AI 執行論醫療 AI 開發及應用〉，《全國律師》，第 30 卷，第 1 期，115 年 1 月，頁 70。

利完成智慧醫療器材產品的查驗登記程序。首先，「人工智慧/機器學習技術之醫療器材軟體查驗登記技術指引」係針對使用 AI/ML 技術的醫療器材明定審查要求，包含軟體概要描述、演算法架構說明、用於模型訓練與驗證的資料描述、資訊安全評估、功能性驗證，以及臨床效能驗證等。此外，也針對較常見的 AI/ML 技術用於電腦輔助偵測（computer-assisted detection devices, CAdE）、電腦輔助診斷（computer-assisted diagnosis devices, CAdx）與電腦輔助分流（computer-assisted triage devices, CAdt）的醫療器材，分別公告「人工智慧機器學習技術之電腦輔助偵測(CAdE)及電腦輔助診斷(CAdx)醫療器材查驗登記技術指引」和「人工智慧機器學習技術之電腦輔助分流(Computer Aided Triage)醫療器材軟體查驗登記技術指引」，說明宣稱不同用途的電腦輔助 AI/ML 醫療器材，其臨床效能驗證時的考量重點²⁹。

為因應醫療器材軟體具備快速更新迭代的特性，衛福部公告「醫療器材軟體上市後變更申請之管理指引」，說明軟體上市後之變更若影響產品本身的效能、用途或使用上的安全有效性時，須辦理許可證變更申請作為判斷原則，協助業者評估軟體上市後何種變更須提出許可證變更申請。而 113 年 9 月，衛福部公告「應用人工智慧/機器學習技術之醫療器材軟體預定變更控制計畫申請要點暨撰寫說明指引」，則進一步導入美國 PCCP 的管理方式，同樣於軟體申請上市時或申請變更時，在產品預期用途/適應症不變的條件下，可同時提交未來軟體預計更新的變更控制計畫，包含預定變更描述、預定變更程序以及影響評估，讓衛福部審查。一旦審查通過，後續的軟體變更只要

²⁹ 滕欣，〈人工智慧醫療器材軟體法規介紹與挑戰〉，《當代醫藥法規月刊》，第 169 期，113 年 1 月，頁 6-7。

業者確認屬計畫書核定範圍，可依預定變更程序執行變更，且留下文件紀錄，則無須頻繁向衛福部提交變更申請。這種預先提交計畫的管理模式，讓業者能在持續優化演算法或模型的同時，避免每次變更都需重新審查，縮短審核時程，促進創新。同時，衛福部亦要求廠商在更新過程中嚴格監控產品風險，確保每次變更不影響既有安全性和效能³⁰。

二、負責任AI執行中心

隨著資訊技術與大數據運算能力的指數級成長，臺灣醫療體系正經歷一場前所未有的轉移，AI 已由單純的實驗室驗證階段，正式轉向深度的臨床整合階段。在這一進程中，臺灣醫療人工智慧的發展已正式跨越了技術導入的初創期，邁入所謂的「治理成熟期」。當前醫療治理的核心戰略，在於如何將抽象的「倫理原則」轉化為具體的「技術與行政實踐」，因此衛福部於 113 年推動「負責任 AI 執行中心」(R-AI Hub)計畫，並參考 WHO 提出使用 AI 於醫療領域的 6 大原則，以及國家科學及技術委員會於當時公布之「人工智慧基本法草案」揭示的 7 大原則，提出 3 大 AI 治理策略，以提高 AI 於臨床應用的透明度與效率，及增進公眾對於 AI 技術在醫療領域應用的信任與接受度³¹。

該中心被賦予 3 大核心任務，首要任務是成立「獨立審查委員會」，這是一個跨專業的協作機制，醫院端須透過此委員會針對每一項欲落地的 AI 產品進行嚴格審核，確保其符合隱私規範、資安標準並具備實質臨床效益，這種跨領域的審查模式能有效過濾掉僅具技術熱情卻缺乏臨床價值的應用，確保技術演進始終對齊醫療品質。第二大任務在於建立透明性指標與可解釋性分析，消除「演算法黑盒子」

³⁰ 同前註，頁 7。

³¹ 吳英志，同註 28，頁 71。

疑慮，將 AI 的開發詳情與侷限性全面公開。第三大任務則是推動「在地測試」與「全生命週期管理」。AI 模型對資料極其敏感，即便通過國際認證的模型，仍可能因臺灣本土資料特性(如盛行率或人種差異)而產生誤差。因此，醫院在導入初期必須使用院內具代表性的標準資料進行在地化測試，確認其性能達到預期³²。

三、醫療機構應用生成式人工智慧指引

我國《人工智慧基本法》已於 115 年 1 月 14 日公布施行，該法採取風險分級的管理思維，其中第 18 條規定，政府應依本法規定，檢討所主管之法規與行政措施；有不符本法規定或無法規可適用者，應自本法施行後 2 年內，完成法規之制(訂)定、修正或廢止，及行政措施之改進。據此，衛福部於 115 年 5 月 29 日發布「醫療機構應用生成式人工智慧指引」，以風險為基礎之管理規範及協助產業訂定指引與行為規範，並就醫療機構生成式 AI 之應用提出行政指導建議，落實「以人為本」與隱私保護、風險治理等基本原則，藉由提供一套實務可行的參考架構，期能推動醫療場域安全、負責任地運用新科技，讓 AI 真正成為臨床決策與照護工作的輔助工具，同時兼顧病人安全、醫療品質與病人隱私，整體精神以「負責任創新」為核心，並落實風險治理與適應性³³。

該指引臚列 6 大風險，包括(一)基礎模型風險；(二)資料來源風險；(三)輸出結果風險；(四)資安攻擊風險；(五)使用者依賴風險；(六)服務中斷風險。為因應上述風險，衛福部進一步提出

³² 李建璋，臺灣醫療人工智慧之負責任實踐：從國際倫理框架到臨床落地治理之全生命週期分析，衛生福利部資訊處，114 年 6 月 2 日，網址：<https://aicenter.mohw.gov.tw/AC/cp-7202-82645-208.html>，最後瀏覽日期：115 年 7 月 31 日。

³³ 衛生福利部，醫療機構應用生成式人工智慧指引，115 年 5 月 29 日，網址：<https://www.mohw.gov.tw/cp-18-86695-1.html>，最後瀏覽日期：115 年 7 月 31 日。

醫療機構導入生成式 AI 的治理原則與管理措施，並提出下列協助機構按生成式 AI 導入生命週期規劃與執行：(一)「導入前評估階段」，醫療機構應指派主責單位或專責人員，負責生成式 AI 系統的風險辨識、評估及分級管理，並建立人工智慧產品與系統清單。指引指出，醫療機構應評估系統資料來源的多元性、時效性與可靠性，同時檢視是否符合《個人資料保護法》、《醫療法》及相關醫事法規規範。此外，系統上線前也應完成資訊安全與資料保護評估，確認資料蒐集、處理、儲存與利用過程的合法性與安全性。(二)「導入與整合階段」，醫療機構應評估生成式 AI 系統與電子病歷、醫院資訊系統及醫學影像傳輸系統等既有系統的整合能力，並進行效能驗證、壓力測試及臨床安全測試，確保系統在實際臨床情境下的輸出品質與安全性。對於高風險應用，則建議採分階段導入方式，先於測試環境驗證後，再逐步擴大至特定科別或臨床場域。此外，指引也要求醫療機構強化供應商管理。未來與 AI 廠商簽訂契約時，應明確規範模型品質、偏誤管理、可追溯性、資料使用權限及資安防護措施等內容，並要求供應商揭露所使用的 LLMs 名稱、版本、部署方式及更新機制，以利後續管理與風險控管。(三)「導入後使用與監管階段」，衛福部強調生成式 AI 應定位為輔助工具，而非取代醫事人員專業判斷。凡涉及臨床判斷、病人安全、病人溝通或醫療紀錄等情境，仍須由具專業資格的醫事人員進行最終確認、審核與負責。醫療機構也應建立持續監測、異常通報與偏誤管理機制，定期檢視系統輸出品質及臨床適用性³⁴。

值得注意的是，指引特別納入近年生成式 AI 常見的提示詞注入攻擊風險，提醒醫療機構建立輸入過濾與異常監測機制，避免惡意指令影響系統輸出內容，進而危及病人安全或造成敏感資訊外洩。在病

³⁴ 同前註。

人權益保障方面，衛福部要求醫療機構以適當方式告知病人及家屬生成式 AI 的參與範圍、用途與限制。若 AI 系統直接與民眾互動，應主動揭露其為 AI 系統，並提醒輸出內容可能存在錯誤或幻覺風險。若醫療照護過程涉及錄音、錄影等 AI 輔助應用，也應事先取得病人或家屬知情同意，若病人明確拒絕，則應停止相關作業³⁵。

伍、問題研析與建議

一、建立完整的 AI 醫療風險分級及管理規範

歐盟 AIA 核心結構在於以風險分級 (Risk based approach) 作為規範強度配置之依據，分為四層風險架構處理 AI 應用，包括 (一) 不可接受風險 (Unacceptable risk)，此類 AI 系統大致被明文禁止，例如社會評分或特定即時遠端生物辨識；(二) 高風險 (High risk)，包括醫療器材、關鍵基礎設施、教育評估等，從設計到上市後監測的全生命週期進行嚴格合規監管；(三) 有限風險 (Limited risk)，如聊天機器人，重點在於透明度義務；(四) 最小或無風險 (Minimal or no risk)，主要透過自律規範或行為準則引導。此一制度特色，在於以不同層級對應不同的監管強度³⁶。

相較之下，我國《人工智慧基本法》第 16 條所建構者，係由數位發展部（下稱數發部）推動風險分類框架，再由各目的事業主管機關據以訂定管理規範。《人工智慧基本法》本身並未如 AIA 明文建立由低至高的分級表，而是在第 5 條第 2 項及第 17 條中賦予「高風險應用」特定法律效果。至於真正具有等級化設計者，仍由各目的事業主管機關訂定。換言之，《人工智慧基本法》的重點，是先確認某一

³⁵ 理律法律事務所，衛福部頒布「醫療機構應用生成式人工智慧指引」，115 年 6 月 26 日，網址：<https://www.leeandli.com/TW/Newsletters/7656.htm>，最後瀏覽日期：115 年 7 月 31 日。

³⁶ 張麗卿，〈AI 基本法下高風險智慧醫療之治理〉，《當代法律》，第 54 期，115 年 6 月，頁 109。

AI 應用是否進入「高風險」類型，若一旦進入，即應依第 17 條啟動責任歸屬、歸責條件以及救濟、補償或保險等制度³⁷。

有論者指出，進行比較法借鏡時，不宜逕將歐盟高風險清單等同於我國的高風險認定標準。歐盟所稱高風險，是其四級架構中的特定層級，並以不可接受風險與有限風險作為上下對照；我國則是在高風險與非高風險的二分結構中，要求各目的事業主管機關進一步細緻化分級及訂定管理方式。尤其在「非高風險」類別內，仍可能存在風險程度差異甚大的應用類型，如何作成有意義的差別處理，將是各機關未來法規調適的重要課題³⁸。

數發部依據《人工智慧基本法》第 16 條第 1 項規定，於 115 年 7 月 7 日發布「人工智慧風險分類框架」，作為我國各目的事業主管機關訂定 AI 風險治理管理規範時，可依循本框架所定操作流程辦理風險識別、評估及應對。本框架有三大重點：第 1 部分用以掌握整體治理架構定位；第 2 部分理解本框架之適用範圍與核心原則；第 3 部分為風險管理之主要操作流程。各機關應依循「盤點應用情境」、「識別風險」、「評估風險」及「應對風險」等四步驟操作流程，進行 AI 應用之風險評估與應對，並據此訂定經管目的事業之管理規範³⁹。

衛福部雖訂有「醫療機構應用生成式人工智慧指引」，列出 6 類風險來源，並規定指派主責單位或人員辨識、控管與管理風險，但相較於國際規範，我國對於風險分級界定似乎較為不足，多屬宣示提醒性質，尤其對於 AI 應用是否屬《人工智慧基本法》所規定之「高風險應用」，並無明確規範，以致無從執行該法第 17 條有關明確其責任

³⁷ 同前註，頁 109。

³⁸ 張麗卿，同註 36，頁 109。

³⁹ 數位發展部，人工智慧風險分類框架，115 年 7 月 8 日，網址：<https://moda.gov.tw/major-policies/ai/governance/19244>，最後瀏覽日期：115 年 7 月 31 日。

歸屬及歸責條件，並建立其救濟、補償或保險機制。爰此，建議主管機關宜進一步參考外國立法例及數發部之「人工智慧風險分類框架」，明確建立完整的 AI 醫療風險分級及管理規範，尤其是高風險 AI 認定程序的具體化，以建構適合我國醫療體系的風險治理模式，並與國際標準接軌。

二、明確 AI 醫療之責任歸屬，並研議救濟、補償或保險機制

AI 一旦進入臨床決策流程，將直接牽動醫師的民刑事責任風險。依 WHO「AI 運用於健康領域的倫理與治理指引」原則，現階段 AI 醫療應居於醫療輔助地位，最終的醫療決策仍由主治醫師綜合病情及本於專業知識定奪⁴⁰。歐盟 AIA 亦有類似的規定。有論者指出，智慧醫療所引發的法律問題，核心不在於醫師是否可以使用 AI，而在於醫師在使用 AI 時應負何種審視、確認與最終判斷義務。醫師固然不能完全依賴 AI 系統，必須依照自己的專業歷練進行最終判斷；但反過來說，若醫師面對的是經認定為高風險且已通過國家審核、具備充分證據基礎的 AI 醫材，其合理信賴的範圍就應受到法律保護，以避免防衛性醫療（Defensive Medicine）蔓延⁴¹。亦有論者指出，演算法易出現所謂的「黑盒子」現象⁴²，為了同時確保病人的安全與權益以及促進醫療的進步，除了醫師必須謹慎使用 AI 外，也有必要合理分配醫療機構與製造商之間的責任，以保障賠償機制的公平性與有效性⁴³。醫療機構對於 AI 系統選用、驗證、教育訓練或流程設計皆應謹慎

⁴⁰ 蕭佳敏，同註 5，頁 90。

⁴¹ 張麗卿，同註 36，頁 111。

⁴² 「黑盒子」現象發生的原因包括：1、不可解釋性(Inexplicability)的存在：未能清楚說明 AI 系統係如何作出決策；2、不可駕馭性(Uncontrollability)的存在：當 AI 本身的學習能力愈來愈強，其所作決策可能超出開發者原有認知或想像，導致出現開發者亦難以駕馭之結果。

⁴³ 朱帝榮、蔡孝誠，〈從黑盒子到新注意義務：重探當代美國 AI 醫療責任之法理基礎〉，《當代法律》，第 46 期，114 年 10 月，頁 131。

處理，否則可能造成管理過失⁴⁴。AI 醫療開發商對於技術的效果確認，不應只在開發階段確保其技術或儀器符合當時科技或專業水準，後續應用階段仍須密切監控結果及效益，持續關注是否偏離合理範圍，產生偏誤，以避免產品責任訴訟⁴⁵。

對於醫療責任分配及醫師專業保護，有論者提出以下建議：第一，於相關法規中明定，醫師使用經主管機關核可並依規上市的 AI 醫材，且依臨床指引與合理程序操作時，得作為判斷其已盡注意義務的重要依據；第二，建立醫療 AI 不良事件通報制度，使醫療機構與業者共同回報 AI 相關事件，作為日後責任認定與系統改善的客觀資料；第三，參酌歐盟 AIA 的人類監督原則，明確化醫師對 AI 輸出結果的審視義務範圍；第四，推動醫療 AI 責任保險或相當的財務擔保機制，使業者、醫療機構與醫師之間，形成較為合理的風險分擔結構⁴⁶。

我國《人工智慧基本法》第 17 條要求政府就高風險 AI 應用明確責任歸屬及歸責條件，並建立救濟、補償或保險機制，此一規定在智慧醫療領域尤具意義。爰此，建議主管機關除應具體化高風險 AI 的認定程序外，對於 AI 醫療的責任歸屬訂定明確的規範，以利釐清醫療責任究竟歸屬於導入 AI 的醫院、做出決策的醫師、AI 開發者、或三者共同承擔，並應研議救濟、補償或保險機制，以保護病患權利。風險控制能力亦可作為各主體責任分配的基準，並分別處理民事、行政及刑事責任。醫師對經核准 AI 的合理信賴得作為注意義務判斷因素，但不宜推導為免責。另宜將模型版本、重要輸入輸出、人工覆核、變更紀錄及不良事件等資料，整合為高風險醫療 AI 的事故可追溯與

⁴⁴ 胡峰賓、翁紹仁，〈人工智慧醫療實務應用下之法制問題探討〉，《全國律師》，第 30 卷，第 1 期，115 年 1 月，頁 11。

⁴⁵ 蕭佳敏，同註 5，頁 92。

⁴⁶ 張麗卿，同註 36，頁 111。

證據保存機制⁴⁷。

三、強化 AI 醫療隱私保護規範

AI 開發涉及真實病人的資料時，隱私是最受重視的價值，需避免資料洩漏，與保護資料提供者的相關權利⁴⁸。AI 為人類帶來前所未有的診療效率與精準度，然而，這場技術躍進的同時也引發了一系列複雜的法律、倫理與安全挑戰，迫使各國政府必須在「促進創新」與「保障病患安全」之間尋求微妙的平衡⁴⁹。

智慧醫療迅速發展之際，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⁵⁰。使用 AI 的醫療機構若未能妥善保護患者健康資訊，造成資訊洩漏或未遵守加密要求，不僅對醫院組織造成影響，還會削弱患者對資訊分享和醫療服務的信任。AI 也會暴露系統的脆弱性，讓惡意攻擊者得以操縱醫療工作流程或利用網路安全防禦中的漏洞，進行犯罪行為。網路犯罪者可能利用 AI 系統篡改醫療記錄、製造虛假的保險申報資料，甚至破壞整個醫院的網路系統⁵¹。

為解決這些問題，有論者提出需要在 AI 全生命週期中實施全面的緩解策略。在「資料收集階段」，可以採用差分隱私(Differential

⁴⁷ 參照附錄張麗卿教授第四點意見

⁴⁸ 蔡甫昌、周昱辰、布嘉俊、莊宇真、詹寶珠，〈生成式 AI 醫學應用之倫理考量〉，《台灣醫學》，第 29 卷，第 2 期，114 年 3 月，頁 131。

⁴⁹ 廖建瑜，〈醫療領域人工智慧之規範模式選擇：從比較法反思台灣人工智慧基本法〉，《全國律師》，第 30 卷，第 1 期，115 年 1 月，頁 35。

⁵⁰ 胡峰賓、翁紹仁，同註 44，頁 6。

⁵¹ 黃維民，同註 1，頁 14。

Privacy) 的保護技術，透過向資料添加統計干擾變數，以隱藏個人身份，同時保留資料的實用性；聯邦學習 (Federated Learning) 也可用來保護病患隱私，允許模型在資料本地化的條件下進行去中心化訓練，例如多家醫院合作使用聯邦學習訓練癌症檢測 AI 模型，無需共享原始患者資訊，即可實現高效能的結果。在「模型開發階段」，對抗性訓練是一種提高模型抗攻擊能力的有效手段，例如通過在訓練期間向模型暴露對抗性樣本，開發者可以提高模型的穩健性，減少臨床部署中的錯誤風險。在「實施階段」，可參考如美國 FDA 的 AI 指導方針或美國國家標準暨技術研究院 (National Institute of Standards and Technology, NIST) 的 AI 風險管理框架，這些規範在問責制和透明度方面可以發揮關鍵作用，強調實際性能監測、持續的風險評估以及利益相關者的合作，以解決新興的隱私與安全問題。透過採取這些措施，醫療機構可以減輕風險，維護公眾信任，並充分發揮 AI 在改善患者結果和提升運營效率方面的潛力⁵²。

我國《人工智慧基本法》對於資訊安全及隱私保護訂有相關的規定⁵³，而「醫療機構應用生成式人工智慧指引」亦提及應完成資訊安全與資料保護評估，並保護病人隱私，惟皆屬概念性的指導。爰此，建議主管機關宜對 AI 醫療的隱私保護建立完整規範，例如個人資料去識別化的保護及加密處理、降低被識別風險、資料管理權限、跨院或跨機構的資料整合……等，以保護病患隱私，並提升 AI 醫療的安

⁵² 黃維民，同註 1，頁 15。

⁵³ 《人工智慧基本法》第 4 條第 3 款規定：「隱私保護與資料治理：應妥善保護個人資料隱私，尊重企業營業秘密，避免資料外洩風險，並採用資料最小化原則；同時在符合憲法隱私權保障之前提下，促進非敏感資料之開放及再利用。」第 4 款規定：「資安與安全：人工智慧研發與應用過程，應建立資安防護措施，防範安全威脅及攻擊，確保其系統之穩健性與安全性。」第 14 條規定：「各目的事業主管機關會商個人資料保護主管機關，在人工智慧研發及應用過程，避免不必要之個人資料蒐集、處理或利用，並應促進個人資料保護納入預設及設計相關措施或機制，以維護當事人權益。」

全與可信賴程度。另應區分個別病人診療、模型訓練與微調、模型驗證、研究二次利用及跨機構資料共享等情境，分別檢視其法律依據與必要性⁵⁴。

四、研議訂定 AI 應用於心理健康領域之管理規範

人類生活與 AI 的連結已包含醫療資訊的提供，看病前先找 AI 問診，已成許多民眾的就醫習慣，有國外研究顯示，每 6 名美國成年人，就有 1 人每月至少向 AI 聊天機器人詢問一次健康相關資訊，這個比例將持續攀升⁵⁵，但也衍生出 AI 是否產生錯誤訊息，導致延誤就醫或錯誤照護決策，進而引發醫病關係緊張及相關法律問題⁵⁶。

有研究指出，AI 在心理治療領域被認為具有潛力，儘管伴隨著重要的倫理與實踐考量，但已被評估為有益的「工具」，包括（一）篩選與診斷：它可以協助進行初步的篩選和診斷，例如它能針對患者描述的症狀提供準確的診斷建議，如抑鬱症、廣泛性焦慮症和社交焦慮症，並具備對心理病理學相關理論的理解；（二）提供治療資訊與建議：它能提供治療選項和方法，雖然在未明確要求下傾向於認知行為療法，但若有明確提示，也能提供其他治療取向的解釋，例如語意治療與存在分析；（三）解釋患者材料：它可以對患者的材料（如夢境）進行解釋，並能從不同的心理治療學派（如心理動力學、系統學、存在分析、個體心理學）提供詮釋，這對於已具心理治療經驗的患者來說，是個獨自處理材料的好機會；（四）提供治療技巧與實踐指導：

⁵⁴ 參照附錄張麗卿教授第五點意見。

⁵⁵ 劉文瑜，向 AI 問診可行嗎？研究：提供資訊不全可能生成錯誤診斷，中央社，115 年 2 月 10 日，網址：<https://www.cna.com.tw/news/ait/202602100110.aspx>，最後瀏覽日期：115 年 7 月 31 日。

⁵⁶ 沈能元、廖靜清，「AI 假醫師」亂亂講！YouTube 深偽影片氾濫 3 大原則防被騙，聯合新聞網，115 年 3 月 24 日，網址：<https://udn.com/news/story/7266/9398429>，最後瀏覽日期：115 年 7 月 31 日。

能夠為治療師提供建議的治療技巧；(五)學習其他治療方法：協助治療師了解不同的心理治療方法。AI 並不是心理師，無法提供心理諮商或醫療診斷，然而，在心理健康的歷程中，有一段很重要、卻常被忽略的前期階段—學習傾聽自己、辨識感受、把內在狀態說出來，這正是 AI 能發揮價值的地方⁵⁷。

雖然 AI 用於心理健康領域有其助益，但也產生了一些隱憂。美國近年發生多起使用者沉迷與 AI 聊天機器人對話，最終不幸輕生，引發家屬對 AI 開發商提出過失致死訴訟的社會悲劇⁵⁸。因此，美國已有許多州政府針對 AI 使用於心理健康領域制定監管或限制法規，伊利諾州(Illinois)於 2025 年 8 月 1 日通過《心理資源健康與監督法》(HB 1806, Wellness and Oversight for Psychological Resources Act, WOPRA)，限制 AI 在心理治療與心理治療決策中的使用以保護患者。該法旨在保護患者免於未受管制且缺乏認證的 AI 產品所造成之風險，同時維護合格且擁有證照之專業執業人員的工作權，該法亦對於近日逐漸受到關注之「青少年心理健康 AI 聊天機器人」風險提供保障。內華達州(Nevada)於 2025 年 6 月 5 日通過 AB 406 法，該法規範了 AI 在心理和行為健康照護領域的應用，禁止提供及推出「能夠進行持有證照之專業心理/行為健康服務」(如心理諮商、心理治療或診斷等)的 AI 系統，同時也禁止 AI 宣稱可以提供上述專業醫療服務，本法同時亦對心理和行為健康照護專業人員如何使用 AI 系統加以限制。而猶他州(Utah)在 2024 年通過《猶他州人工智慧政策法》(Utah' s Artificial Intelligence Policy Act, UAIPA)，除對「心

⁵⁷ 甘翠瑜、邱采芊、張聖婷、李明峰，〈研究：AI 輔助心理治療能改善憂鬱及焦慮症狀！〉，《輔導季刊》，第 61 卷，第 4 期，114 年 12 月，頁 37。

⁵⁸ 劉怡廷，美 14 歲少年疑因沉迷與 AI 聊天導致自殺 母提告控科技公司過失致死，公視新聞網，113 年 10 月 24 日，網址：<https://news.pts.org.tw/article/720988>，最後瀏覽日期：115 年 7 月 31 日。

理健康聊天機器人」訂出定義與規範，並要求揭露、隱私與資料分享限制、廣告與定位限制等⁵⁹。

因此有專家提醒，心理治療不同於一般生理醫療，AI 雖可彌補現實中無法即刻安排心理治療的需求，但人類的問題錯綜複雜，仍需要不同取向的心理治療來協助解救情緒方面的問題。心理學倫理要求「不傷害」、「自主原則」與「保密義務」，而心理治療的核心在於治療聯盟（Therapeutic Alliance）⁶⁰、情感支持、直覺與創造力，這些都是 AI 目前無法實現的。AI 現階段仍然無法替代面對面的真人心理治療，病患仍需及時尋求專業心理師的協助，經過正確的診斷與遵照醫囑接受治療，才能有良好的效果⁶¹。

WHO 提醒，各國應建立 AI 心理健康治理架構，避免 AI 在缺乏監督下提供建議，如何建立兼顧病人權益、醫療安全及 AI 創新的法律制度，已成為世界各國共同面臨的重要課題⁶²。我國目前針對 AI 應用於心理健康領域尚無專法或規範，爰此，建議主管機關在《人工智慧基本法》及《醫療機構應用生成式人工智慧指引》之基礎上，研議於相關法規如《醫療法》、《心理師法》或《醫療器材管理法》等增訂 AI 應用與輔助的專章或條文，包括：明確劃分「AI 心理輔助工具」與「專業心理治療」之界線；規範心理師於臨床使用 AI 工具時的法

⁵⁹ 焦汝安，美國伊利諾州(Illinois)於 2025 年 8 月初通過《心理資源健康與監督法》(WOPRA)，禁止非專業證照人士或 AI 提供心理健康之治療或服務，Stli，114 年 9 月 30 日，網址：<https://www.biotechlaw.org.tw/activity/posts/109>，最後瀏覽日期：115 年 7 月 31 日。

⁶⁰ 治療聯盟（Therapeutic Alliance）指的是心理師（或醫師）與案主（或患者）之間，為了達成療癒目標而建立的合作關係。這個核心概念包含三個重要元素：目標共識、任務分工與情感連結。治療聯盟的建立需要治療師展現出真誠的情感共鳴和同理心，而這些都是 AI 目前無法真正實現的。即使 AI 可以模擬出同理心的語言，這種模擬也缺乏真實的情感基礎。

⁶¹ 董氏基金會心理衛生中心，〈人工智慧運用在諮商領域中的倫理議題：以聊天機器為例〉，《臺灣憂鬱症防治協會通訊》，第 22 卷，第 5 期，112 年 10 月，頁 8。

⁶² WHO, Towards responsible AI for mental health and well-being: experts chart a way forward, Mar. 20, 2026, available at: <https://www.who.int/news/item/20-03-2026-towards-responsible-ai-for-mental-health-and-well-being--experts-chart-a-way-forward?>, last visited on Jul. 31, 2026.

定程序；制訂 AI 心理輔助系統審查制度，或針對心理諮商與治療類別之 SaMD 建立專門審查指引，依據軟體的「自主程度」與「風險高低」實行分級管理；任何 AI 心理健康系統必須設置「高風險（如自殘、自殺意念）的自動識別與即時人工介入或轉介專線（如 1925 安心專線）的強制機制；心理師在輔助診斷中使用 AI 時，也應讓患者確實知情與同意，並保護隱私權；醫師、醫療機構及 AI 開發商也應隨時共同檢視 AI 程式在心理健康應用的影響評估和監測，讓 AI 與人類心理師形成一種協同發展的關係，共同推動心理諮詢領域的進步。

陸、結論

AI 持續的蓬勃發展已成為時代趨勢，在這股潮流中，我們應思考如何妥善利用而非被動接受其影響。AI 為醫療領域帶來精準診斷與廣泛應用，提升了醫療的品質及效率，但也有潛在的隱私風險和倫理考量。AI 的發展必須以人為本，並以造福人類為目標，將技術應用於醫療服務的同時，應確保道德責任，才能讓醫療領域持續進步。因此，我國必須建置完善的法制規範，才能有助於 AI 於醫療上的使用，謹提出下列建議，俾供委員問政參考：

- 一、建立完整的 AI 醫療風險分級及管理規範。
- 二、明確 AI 醫療之責任歸屬，並研議救濟、補償或保險機制。
- 三、強化 AI 醫療隱私保護規範。
- 四、研議訂定 AI 應用於心理健康領域之管理規範。

參考文獻

一、期刊

- 1、甘翠瑜、邱采芊、張聖婷、李明峰，〈人工智慧運用在諮商領域中的倫理議題：以聊天機器人為例〉，《輔導季刊》，第 61 卷，第 4 期，114 年 12 月，頁 35-47。
- 2、朱帝縈、蔡孝誠，〈從黑盒子到新注意義務：重探當代美國 AI 醫療責任之法理基礎〉，《當代法律》，第 46 期，114 年 10 月，頁 127-132。
- 3、吳英志，〈從負責任 AI 執行論醫療 AI 開發及應用〉，《全國律師》，第 30 卷，第 1 期，115 年 1 月，頁 70-76。
- 4、周廼寬，〈醫療人工智慧時代下的資安風險、倫理治理與制度建構—從臺灣近年醫療資安事件談「負責任 AI」的關鍵基石〉，《消費者報導雜誌》，第 542 期，115 年 6 月，頁 27-28。
- 5、胡峰賓、翁紹仁，〈人工智慧醫療實務應用下之法制問題探討〉，《全國律師》，第 30 卷，第 1 期，115 年 1 月，頁 2-14。
- 6、苗光磊，〈人工智慧技術應用於醫療領域所衍生之隱私權保護的法律規制〉，《全球知識發展期刊》，第 2 卷，第 4 期，113 年 12 月，頁 1-25。
- 7、張冠群，〈醫療人工智慧的責任、監理與責任保險問題：歐盟與美國法制之初探及責任保險制度在設計之芻議〉，《全國律師》，第 30 卷，第 1 期，115 年 1 月，頁 57-69。
- 8、張麗卿，〈AI 基本法下高風險智慧醫療之治理〉，《當代法律》，第 54 期，115 年 6 月，頁 106-112。
- 9、黃維民，〈從醫管專業的觀點探討生成式醫療人工智慧的倫理與規範〉，《電腦稽核》，第 53 期，115 年 2 月，頁 4-24。

- 10、董氏基金會心理衛生中心，〈人工智慧運用在諮商領域中的倫理議題：以聊天機器人為例〉，《臺灣憂鬱症防治協會通訊》，第 22 卷，第 5 期，112 年 10 月，頁 8-9。
- 11、廖建瑜，〈醫療領域人工智慧之規範模式選擇：從比較法反思台灣人工智慧基本法〉，《全國律師》，第 30 卷，第 1 期，115 年 1 月，頁 16-47。
- 12、滕欣，〈人工智慧醫療器材軟體法規介紹與挑戰〉，《當代醫藥法規月刊》，第 169 期，113 年 11 月，頁 1-14。
- 13、蔡甫昌、周昱辰、布嘉俊、莊宇真、詹寶珠，〈生成式 AI 醫學應用之倫理考量〉，《台灣醫學》，第 29 卷，第 2 期，114 年 3 月，頁 129-137。
- 14、蕭佳敏，〈運用人工智慧技術於醫療的法律風險與隱憂－利弊互現〉，《靜宜法學》，第 13 期，113 年 12 月，頁 61-99。
- 15、戴于揚、陳哲民、吳逸帆、吳欣潔、郭冠良，〈論 2024 年 WHO 發表之「人工智慧於健康領域之倫理與治理」與台灣現況〉，《台灣家庭醫學雜誌》，第 34 卷，第 3 期，113 年 9 月，頁 136-143。

二、網路資源

（一）中文網站

- 1、ReBlood，AI 醫療真的都是優點嗎？AI 醫療缺點及挑戰大曝光，113 年 11 月 21 日，網址：<https://rebloodgroup.com/ai-pros-cons/>，最後瀏覽日期：115 年 7 月 31 日。
- 2、工研院產業學院，AI 智慧醫療是什麼？一篇文帶你了解台灣智慧醫療的現況，工研院產業學習網，111 年 7 月 11 日，網址：

<https://college.itri.org.tw/Info/InfoData/1d549534-07c6-4407-b1de-d5a04ddd665c>，最後瀏覽日期：115年7月31日。

- 3、李永健，全球AI醫療照護與器材發展趨勢探討，IEK產業情報網，114年6月12日，網址：https://ieknet.iek.org.tw/iek-rpt/rpt_more.aspx?rpt_idno=643636041，最後瀏覽日期：115年7月31日。
- 4、李建璋，臺灣醫療人工智慧之負責任實踐：從國際倫理框架到臨床落地治理之全生命週期分析，衛生福利部資訊處，114年6月2日，網址：<https://aicenter.mohw.gov.tw/AC/cp-7202-82645-208.html>，最後瀏覽日期：115年7月31日。
- 5、呂政諺，歐盟發布人工智慧法、醫療器材法與體外診斷醫療器材法協同適用問答集，Stli，114年7月，網址：<https://stli.iii.org.tw/article-detail.aspx?tp=1&d=9376&no=64>，最後瀏覽日期：115年7月31日。
- 6、吳振吉，AI革命下的醫療新紀元：應用潛力與法律挑戰，天下雜誌，113年4月25日，網址：<https://futurecity.cw.com.tw/article/3399>，最後瀏覽日期：115年7月31日。
- 7、沈能元、廖靜清，「AI假醫師」亂亂講！YouTube深偽影片氾濫 3大原則防被騙，聯合新聞網，115年3月24日，網址：<https://udn.com/news/story/7266/9398429>，最後瀏覽日期：115年7月31日。
- 8、施雅薰，全美各州醫療委員會聯合會發布人工智慧（AI）治理指引，並要求醫師為AI之利用結果負最終責任，Stli，113年9月，網址：<https://stli.iii.org.tw/article-detail.a>

spx?tp=1&d=9239&no=64，最後瀏覽日期：115年7月31日。

- 9、施雅薰，世界衛生組織發布歐洲區域人工智慧於醫療系統準備情況報告，責任規則為最重要之關鍵政策因素，Stli，115年1月18日，網址：https://stli.iii.org.tw/article-detail.aspx?no=65&tp=1&d=9442#_ftnl，最後瀏覽日期：115年7月31日。
- 10、陳芳毓，智慧醫療懶人包》八張圖，一次搞懂智慧醫療的定義、應用與台灣的挑戰，天下雜誌，112年1月1日，網址：<https://futurecity.cw.com.tw/article/1916>，最後瀏覽日期：115年7月31日。
- 11、陳昱安，人工智慧醫療器材該如何監管？以美國經驗為例，DSET，113年4月19日，網址：<https://dset.tw/research/00010/>，最後瀏覽日期：115年7月31日。
- 12、理律法律事務所，衛福部頒布「醫療機構應用生成式人工智慧指引」，115年6月26日，網址：<https://www.leeandli.com/TW/Newsletters/7656.htm>，最後瀏覽日期：115年7月31日。
- 13、曾柏諺，人工智慧在醫療領域的應用與挑戰－資訊科技在生醫領域擦出新火花，中國醫藥大學學生會，115年7月20日，網址：<https://www.twcmusa.org/column/%E4%BA%BA%E5%B7%A5%E6%99%BA%E6%85%A7%E5%9C%A8%E9%86%AB%E7%99%82%E9%A0%98%E5%9F%9F%E7%9A%84%E6%87%89%E7%94%A8%E8%88%87%E6%8C%91%E6%88%B0%EF%BC%8D%E8%B3%87%E8%A8%8A%E7%A7%91%E6%8A%80%E5%9C%A8%E7%94%9F/>，最後瀏覽日期：115年7月31日。

- 14、焦汝安，美國伊利諾州(Illinois)於2025年8月初通過《心理資源健康與監督法》(WOPRA)，禁止非專業證照人士或AI提供心理健康之治療或服務，Stli，114年9月30日，網址：<https://www.biotechlaw.org.tw/activity/posts/109>，最後瀏覽日期：115年7月31日。
- 15、數位發展部，人工智慧風險分類框架，115年7月8日，網址：<https://moda.gov.tw/major-policies/ai/governance/19244>，最後瀏覽日期：115年7月31日。
- 16、劉文瑜，向AI問診可行嗎？研究：提供資訊不全可能生成錯誤診斷，中央社，115年2月10日，網址：<https://www.cna.com.tw/news/ait/202602100110.aspx>，最後瀏覽日期：115年7月31日。
- 17、劉怡廷，美14歲少年疑因沉迷與AI聊天導致自殺 母提告控科技公司過失致死，公視新聞網，113年10月24日，網址：<https://news.pts.org.tw/article/720988>，最後瀏覽日期：115年7月31日。
- 18、衛生福利部，醫療機構應用生成式人工智慧指引，115年5月29日，網址：<https://www.mohw.gov.tw/cp-18-86695-1.html>，最後瀏覽日期：115年7月31日。

(二) 外文網站

- 1、European Commission, AI Act, Aug. 1, 2025, available at : <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>? last visited on Jul. 31, 2026.

- 2、FDA, Artificial Intelligence in Software as a Medical Device, available at : <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-software-medical-device>, last visited on Jul. 31, 2026.
- 3、WHO, Ethics and governance of artificial intelligence for health, Jun. 28, 2021, available at : <https://www.who.int/publications/i/item/9789240029200>, last visited on Jul. 31, 2026.
- 4、WHO, Towards responsible AI for mental health and well-being: experts chart a way forward, Mar. 20, 2026, available at : <https://www.who.int/news/item/20-03-2026-towards-responsible-ai-for-mental-health-and-well-being--experts-chart-a-way-forward?>, last visited on Jul. 31, 2026.

附錄：「人工智慧應用於醫療領域法制問題研究」專題研究報告（初稿）

座談會紀錄及參採情形

時間：115 年 8 月 25 日（星期二）下午 2 時 30 分

地點：立法院法制局 305 會議室

主席：陳組長宏明

紀錄：黃嘉文

參加人員：

一、學者專家

實踐大學法學院 張教授麗卿

二、衛生福利部

醫事司 簡任技正 呂念慈

專員 賴韻如

食品藥物管理署 高級審查員 陳泰龍

心理健康司 科長 呂素蘭

研究員 余培瑋

資訊處 科長 游子佳

三、本局出席人員

趙研究員俊祥

李副研究員志遠

陳副研究員育靖

發言要點：

實踐大學法學院張教授麗卿：

一、報告在「肆、我國 AI 應用於醫療領域之相關規範」第一項醫療器材管理法中，已介紹我國 AI／ML 醫療器材軟體的預定變更控制計畫，並說明在產品預期用途或適應症不變的情形下，業者得預先提出軟體更新的變更控制計畫，經核定後依核定範圍執行。此項制度可作為處理特定醫療 AI 上市後預定變更的基礎。惟 AI 醫療器材可能因資料更新、模型微調、參數調整或部署環境改變而影響系統性能，仍有必要進一步釐清何種模型更新屬於重大變更。若更新已影響預定用途、適用族群、臨床效能、安全性或人為監督能力，或因而產生新的重大風險，即應依現行醫療器材法制及核定的變更控制計畫，判斷是否須重新驗證或辦理變更。如 AI 應用的風險性質因更新而有實質變化，目的事業主管機關亦宜重新檢視其風險程度與相應管理措施。醫療機構則應掌握實際部署的模型版本、更新日期及主要性能變化，以利事故發生後釐清風險發生的階段。建議：報告可在既有預定變更控制計畫的介紹後，補充模型重大變更的判斷、再驗證或變更程序，並說明醫療機構應保存實際部署版本及更新紀錄，使上市後監理與事故責任判斷相互銜接。

二、報告在「肆、我國 AI 應用於醫療領域之相關規範」第三項，已介紹衛福部於 2026 年 5 月 29 日函頒的「醫療機構應用生成式人工智慧指引」，內容包括生命週期管理、資訊安全、資料保護、風險分級、版本控制、持續監測及病人告知等事項。就導入後的使用與監管，指引並將生成式 AI 定位為輔助工具，涉及臨床判斷時，仍由醫事人員進行最終確認。現行指引已有一定規範基礎，惟其適用範圍仍有補充空間。首先，報告未就 AI Agent 另行討論。現行指引雖已定義 AI Agent，但考量其具備自主決策

及採取行動的特性，可能涉及較高的病人安全、醫療責任及法令遵循風險，因此暫不列入適用對象。當 AI 由提供資訊或建議，進一步發展為自主或半自主執行醫療相關任務時，僅以醫事人員覆核輸出作為主要控制方式是否足夠，仍有檢討必要。其次，指引已要求醫療機構適當告知病人及家屬生成式 AI 的參與範圍、用途與限制。AI 系統如直接與民眾互動，應揭露其 AI 身分。醫療照護過程如涉及錄音、錄影等 AI 輔助應用，則應事先取得病人或家屬的知情同意。惟不同 AI 使用情境對病人權益的影響程度並不相同，告知及同意要求仍有進一步區分的必要。建議：報告可在指引介紹部分補充 AI Agent 目前未納入適用範圍所形成的規範缺口。至於病人告知，可依 AI 參與醫療決策的程度及是否直接與病人互動加以分層。僅用於一般行政作業者，原則上不另生醫療同意問題。實質參與診斷、治療或重大臨床決策者，則宜說明 AI 的角色、主要限制及專業人員的覆核機制。涉及直接互動或額外敏感資料蒐集時，再提高資訊揭露與同意要求。

三、報告在「伍、問題研析與建議」第一項「建立完整的 AI 醫療風險分級及管理規範」中，已說明我國並未如歐盟 AIA 直接建立四級風險表，而係由數發部依《人工智慧基本法》第 16 條提出風險分類框架，再由各目的事業主管機關依所管領域訂定風險管理規範，此部分說明大致妥當。惟《人工智慧基本法》第 18 條另要求政府檢討主管法規及行政措施，如有不符合基本法規定或無法規可資適用之情形，應於施行後 2 年內完成制（訂）定、修正、廢止或行政措施的調整。就醫療領域而言，衛福部除可透過指引處理現階段的實務需求外，仍宜檢視《醫療法》、《醫師法》、《醫療器材管理法》及相關子法，區分既有規範足以處理的事項與尚

待補充之處，並選擇適當的規範形式。此外，報告已指出，醫療機構應用生成式人工智慧指引雖整理 6 類風險來源，但對何種醫療 AI 屬於《人工智慧基本法》所稱高風險應用，仍欠缺較具體的判斷標準。數發部人工智慧風險分類框架採「盤點應用情境、識別風險、評估風險、應對風險」的操作程序。衛福部可依《人工智慧基本法》第 5 條所列保護利益，並參酌該框架對嚴重危害的評估方式，發展醫療領域的具體判斷因素。判斷時可考量 AI 是否直接影響診斷、治療或其他重大醫療決策，錯誤結果是否可能造成生命、身體的重大或不可逆損害，醫事人員是否仍具有實質覆核及介入可能，模型是否存在持續更新或資料偏差等動態風險，以及使用情境是否涉及兒少、高齡者、精神疾病患者或其他較脆弱的群體。上述因素係醫療領域具體化的判斷指標，並非《人工智慧基本法》已明文列舉的法定要件。報告在風險分級、責任與保險、隱私保護及心理健康 AI 等部分提出多項管理措施，惟尚未進一步區分各項措施所應採取的規範形式。《人工智慧基本法》第 16 條及第 17 條主要課予政府制度建構義務，並未使具體管制措施對醫療機構、醫事人員或 AI 業者發生直接的強制效力。若未來欲將資訊揭露、通報、紀錄保存、強制責任保險、禁止特定 AI 使用或行政處罰等事項轉化為法定義務，仍應依其內容及對人民權益的影響，檢視法律或法規命令的授權基礎。另本項正文記載數發部人工智慧風險分類框架於 115 年 7 月 7 日發布，但註 39 載為 7 月 8 日。建議：報告可在第 1 項建議中一併交代《人工智慧基本法》第 16 條至第 18 條的關係，並補充醫療高風險 AI 的判斷因素與辨識程序。對擬採強制方式的管理措施，則宜進一步說明其法源層級與授權基礎。另人工智慧風險分

類框架的發布日期宜依正式公告統一修正為 115 年 7 月 7 日。

四、報告在「伍、問題研析與建議」第 2 項「明確 AI 醫療的責任歸屬，並研議救濟、補償或保險機制」中，已將醫師、醫療機構及 AI 開發商納入分析，也提及醫療機構的系統選用、驗證、教育訓練及流程設計，以及開發商持續監控系統效能與偏誤等問題。責任分配仍可依各主體實際掌握的資訊與風險控制能力進一步區分。開發者或供應者主要掌握演算法設計、訓練資料品質、已知限制揭露、資安及版本更新。醫療機構則負責採購審查、在地驗證、權限管理、教育訓練、工作流程設計及持續監測。醫事人員的責任，主要發生於具體診療過程中的專業判斷、覆核及必要介入。如此區分，較能避免將系統設計或組織管理上的風險集中由臨床使用者承擔，也與《人工智慧基本法》第 17 條的制度方向相符。報告另引述論者指出，醫師使用經主管機關核准並依規上市的 AI 醫材，且遵循臨床指引及合理程序操作時，可作為判斷是否已盡注意義務的重要資料。此項見解可供制度設計參考，但不宜解為使用經核准 AI 即當然免責。醫師固不得盲目依賴 AI，惟其對經核准且具有相當證據基礎的系統所為合理信賴，仍應作為個案判斷注意義務時的斟酌因素。民事損害賠償、醫療機構的行政管理責任與醫事人員的刑事責任，其規範目的及歸責基礎並不相同，宜分別處理。刑事過失責任仍應依行為時的注意義務、結果可預見性及可避免性判斷。責任制度能否實際運作，也與事故後是否具有足以追溯系統運作情形的紀錄有關。報告及衛福部指引已提及模型版本、部署方式、更新機制、異常通報及持續監測，並引述建立醫療 AI 不良事件通報制度的建議。事故發生後，如無法確認當時使用的模型版本、主要輸入與輸出、系統

更新情形、醫事人員是否覆核，以及供應商是否曾通知已知風險，責任歸屬與因果關係即難以判斷。建議：報告在責任部分可進一步以風險控制能力作為各主體責任分配的基準，並分別處理民事、行政及刑事責任。醫師對經核准 AI 的合理信賴得作為注意義務判斷因素，但不宜推導為免責。另宜將模型版本、重要輸入輸出、人工覆核、變更紀錄及不良事件等資料，整合為高風險醫療 AI 的事故可追溯與證據保存機制。

五、報告在「伍、問題研析與建議」第三項「強化 AI 醫療隱私保護規範」中，已討論病歷、醫學影像、基因資料及生理音檔等敏感健康資訊，並提出去識別化、加密、資料管理權限及跨院或跨機構資料整合等措施。除資訊外洩風險外，資料用途變更亦宜納入討論。AI 訓練、微調、驗證及持續改善，均可能使用原先為診療目的所蒐集的資料。後續利用是否仍在原蒐集目的的範圍內，仍須依個資法及相關醫療法規判斷其法律依據、必要性與比例性，不宜僅因用途涉及醫療或研究即逕認合法。《人工智慧基本法》第 14 條關於避免不必要個資利用及將個人資料保護納入預設與設計的要求，亦可作為規範參考。建議：報告可在隱私保護之外，補充資料目的外利用的法制問題，並區分個別病人診療、模型訓練與微調、模型驗證、研究二次利用及跨機構資料共享等情境，分別檢視其法律依據與必要性。

六、報告在「伍、問題研析與建議」第四項「研議訂定 AI 應用於心理健康領域之管理規範」中，已就 AI 心理輔助、專業心理治療、心理治療類 SaMD、高風險自傷或自殺情境，以及人工介入與轉介等問題提出建議。心理健康 AI 確有較高的治理需求，惟是否有必要另行制定專法，仍可保留討論。人工智慧基本法第 5 條已

揭示兒少最佳利益原則，高風險 AI 產品或系統經主管機關依法認定後，亦有相應警示要求。建議：報告可保留心理健康 AI 的獨立討論，但對另行制定專法採較保留立場。現階段宜優先將兒少、精神健康、自傷或自殺風險、高度情緒依賴，以及直接面向病人的 AI 互動納入醫療高風險評估，再依風險程度設計 AI 身分揭露、人工介入、危機轉介及敏感資料保護等要求。

七、報告在我國法制及「伍、問題研析與建議」4 項建議中，主要討論醫療機構、醫師、AI 開發商與醫療 AI 產品，尚未另行處理政府機關運用 AI 執行醫療相關業務的情形。《人工智慧基本法》第 19 條已規定，政府使用 AI 執行業務或提供服務時，應進行風險評估、規劃因應措施，並依業務性質訂定使用規範或內控管理機制。建議：報告可增列政府使用醫療 AI 的討論。日後如將 AI 導入健保給付審查、醫療必要性判斷、公共衛生風險預測或醫療資源配置，除風險評估及內控外，宜特別檢視是否需要人工覆核、理由說明、錯誤更正及申訴等程序保障，以避免 AI 使用直接影響人民的給付權益及醫療可近性而欠缺救濟途徑。

參採情形：

- 一、第一點及第二點意見，因報告第肆項內容係針對我國目前 AI 應用於醫療領域之相關規範，蒐集文獻資料彙整陳述，爰維持本報告內容，所提建議事項錄供參考。
- 二、第三點意見，有關註 39 之日期係參考數發部網站內容，已參採修正，至於其他建議事項已於報告中詳述。
- 三、第四點及第五點意見，已參採修正相關內容。
- 四、第六點及第七點意見，涉及層面較廣，且國內就 AI 應用於醫療

領域相關議題的討論尚處於萌芽階段，可供參考資料有限，故所提建議事項錄供參考。

衛生福利部心理健康司：

針對本報告問題研析與建議第四項、「研議訂定 AI 應用於心理健康領域之管理規範」所撰內容，意見茲述如下：

一、有關報告第 29 頁第二段內容，本司對報告引用各方文獻並概要回顧 AI 於心理治療領域功能及角色，敬表尊重，如同報告所述「AI 並不是心理師，無法提供心理諮商或醫療診斷」、「心理治療的核心在於治療聯盟（Therapeutic Alliance）、情感支持、直覺與創造力，這些都是 AI 目前無法實現的」，本司認為前開論述係基於心理治療乃自奧地利神經科醫師西格蒙德·佛洛伊德奠定精神分析學派以降，均以「作為自然人之分析者與作為自然人之被分析者之間所建立的治療性關係」為其本質性之定義，換言之，即使「非人對自然人」雖亦可能產生主觀上「療癒感」或「感受到情緒支持」，其性質上仍屬於「一般心理健康促進措施」。爰請貴局於本報告研討有關 AI 應用心理健康領域之管理規範議題時，宜依循國內外醫療及臨床理論與實務之經驗，於用語概念上予以統一，定明「由醫事人員執行之診察、診斷與治療及其輔助決策或治療工具」與「由 AI 應用程式生成擬人化之心理健康促進建議內容」之差異，避免使用「心理治療建議」（第 31 頁）這類較不精確之用語，防止閱聽者對之產生誤解。

二、有關報告第 29 頁第一段內容一節：

（一）AI 開發商經由所製作之 AI 提供生成式內容誘導民眾產生自殺行為之監管機制一事，查我國《自殺防治法》第 16 條規

定，宣傳品、出版品、廣播、電視、網際網路或其他媒體，不得報導或記載下列事項：1. 教導自殺方法或教唆、誘使、煽惑民眾自殺之訊息。2. 詳細描述自殺個案之自殺方法及原因。3. 誘導自殺之文字、聲音、圖片或影像資料。4. 毒性物質或其他致命性自殺工具之銷售情報。5. 其他經中央主管機關認定足以助長自殺之情形。又前開「網際網路或其他媒體」之範疇，自包含由各事業單位製作並公開於網際網路或其他媒體平臺供民眾取用之 AI 程式及所生成之內容；倘經由直轄市、縣（市）主管機關查有違反前開第 16 條規定者，即依同法第 17 條第 2 項規定，處負責人及相關行為人新臺幣（下同）10 萬元以上 100 萬元以下罰鍰，並得沒入前條規定之物品、令其限期移除內容、下架或其他必要之處置；屆期不履行者，得按次處罰，實務上並無窒礙難行之處。

（二）再查我國《心理師法》第 42 條第 1 項規定，已明定未取得臨床心理師或諮商心理師資格，擅自執行臨床心理師或諮商心理師業務者，處 2 年以下有期徒刑，得併科 3 萬元以上 15 萬元以下罰金。又同法第 27 條第 2 項規定，非心理治療所或心理諮商所，不得為心理治療或心理諮商廣告。爰由各事業單位製作並公開於網際網路或其他媒體平臺供民眾取用之 AI 程式及所生成之內容，如有廣告宣稱或實質上涉及執行心理師法定業務等情，除直轄市、縣（市）主管機關得予裁處行政罰鍰及令限期改善外，本部及直轄市、縣（市）主管機關均得依刑事訴訟法向該單位所在地檢調機關告發，以維護民眾健康權益，實務上亦無窒礙難行之處。

三、報告第 31 頁第二段內容一節：

(一) 有關建請「明確劃分『AI 心理輔助工具』與『專業心理治療』之界線」一節：本部業於 114 年 12 月 15 日以衛部心字第 1141763430 號函釋明有關使用 AI 人工智慧執行疑涉《心理師法》所定業務及相關廣告之判斷準則（衛生福利法規檢索系統連結：<https://gov.tw/rSo>），又《心理師法》第 13 條及第 14 條所定心理衡鑑、心理諮商與心理治療業務，均為不確定性法律概念，其學說分類上屬「經驗性不確定法律概念」，依司法院釋字第 545 號解釋之意旨略以，其涵義於個案中並非不能經由適當組成之機構依其專業知識及社會通念加以認定及判斷，並可由司法審查予以確認，則與法律明確性原則尚無不合，本部亦於 113 年 1 月 15 日以衛部心字第 1131760083 號函釋明「心理諮詢」與「心理治療／心理諮商」之定義及區別在案（衛生福利法規檢索系統連結：<https://gov.tw/CNV>），實務上尚無窒礙難行之處，建議不宜於法令明定。

(二) 有關建請「規範心理師於臨床使用 AI 工具時的法定程序」及「心理師在輔助診斷中使用 AI 時，也應讓患者確實知情與同意，並保護隱私權」一節：心理師執行心理衡鑑、心理諮商及心理治療業務，係依《心理師法》第 13 條及第 14 條為之，是類法律行為之本質，係對受服務對象進行「醫事行為」，並非行政機關依「法定程序」所為行政行為。爰如於法令明確規範心理治療服務之操作方式，除有過度限制職業自由及臨床專業發展外，亦將於違法性審查上遭遇相當巨大的困難。爰心理師運用傳統心理衡鑑及測驗工具、新進之各類資通訊科技及 AI 應用程式時，除依現行《醫療法》、《心

理師法》、《個人資料保護法》及資通安全相關規定辦理外，其餘臨床服務操作事宜，應回歸臨床專業判斷、遵循實證研究及專業倫理辦理。

(三) 建請「制訂 AI 心理治療系統審查制度，或針對心理諮商與治療類別之 SaMD 建立專門審查指引，依據軟體的『自主程度』與『風險高低』實行分級管理」一節：有關假設將 AI 應用程式視為代替心理師執行法定業務而衍生相關疑義，及違反我國《心理師法》之分析，同上所述。至有關「輔助執行心理治療工具」於醫療器材管理法之分級管理及建立審查指引，尚涉前開法令所定實體要件及程序事宜，宜洽本部食品藥物管理署回應。

(四) 有關建請「任何 AI 心理健康系統必須設置高風險(如自殘、自殺意念)的自動識別與即時人工介入或轉介專線(如 1925 安心專線)的強制機制」一節：網際網路或各類媒體之系統平臺，針對自殺想法之言論內容設置自動識別與即時介入之強制機制一項，高度涉及人民言論自由、通訊隱私權益，且恐有違反《通訊保障及監察法》相關規定外，亦有文獻回顧研究顯示，AI 演算法於應用上囿於技術發展水準，本身固有誤報、漏報，或對特定群體可能產生歧視性評估結果並衍生法律責任，且如何於各類措施上確保最小侵害原則之下，最大化行善效益並踐行不傷害原則之倫理，均不無疑義。爰本部將依《自殺防治法》第 9 條第 2 項第 8 款規定，持續協助傳播媒體及網際網路平臺遵守自殺新聞報導原則、建立自律機制，並依同法第 11 條第 1 項規定，協助前開各類網際網路系統平臺，自律導入心理健康及自殺防治相關資源，俟

客服人員或管理者知悉其平臺使用者有自殺行為情事時，依循警政署會同本部訂定之「網路平臺業者發現網路自殺訊息書面報案表」及「警察機關受理網路平臺業者發現網路自殺報案處理流程圖」，向使用者所在地之警察機關報案請求及時協助。

- (五) 有關「醫師、醫療機構及 AI 開發商也應隨時共同檢視 AI 程式在心理健康應用的影響評估和監測」一節：依現行資通訊科技及臨床實證相關研究發展情形，尚難僅依據網際網路平臺呈現之言論內容，推斷是類內容得代表此人整體之精神或心理健康狀態，且自殺行為係多元因素共同作用之結果，爰除《自殺防治法》第 11 條已明定相關業務人員知悉自殺行為之通報義務，及同法第 16 條亦明文禁止各類媒體報導或記載是類不當自殺訊息外，醫師、醫療機構及 AI 開發商亦有遵循且不得違反我國《醫療法》、《醫師法》及《心理師法》等相關義務，據以確保病人安全及民眾健康權益，故宜進一步釐清本報告建請針對「心理健康應用的影響評估和監測」之具體標的為何。

參採情形：

- 一、第一點意見，已參採修正。
- 二、第二點意見係主管機關就現行法律規範及實務作法補充說明，錄供參考。
- 三、第三點意見係建議醫師、醫療機構及 AI 開發商應共同隨時留意檢視 AI 程式在心理健康應用的發展，以隨時評估 AI 在發展過程中對於心理健康應用的建議是可行的，爰維持本報告內容。

衛生福利部資訊處：

有關報告第 20 頁「負責任 AI 執行中心」一節，為使內容更完整呈現本部醫療 AI 治理政策及實際推動情形，本處建議酌予補充說明如下：

- 一、本部推動負責任 AI 執行中心，主要係協助醫療機構建立醫療 AI 導入及應用之治理機制，並以「資訊安全及隱私保護」、「應用透明性」及「AI 全生命週期持續監測」為三大治理重點。參與醫療機構透過成立智慧醫療委員會或相關治理團隊，訂定院內智慧醫療管理規範，建立單一服務窗口、標準化申請及審查流程，並就 AI 系統之應用目的、適用範圍、驗證結果、效能指標、使用限制及維護機制等重要資訊進行適當揭露。
- 二、在 AI 系統導入後，醫療機構亦應持續掌握實際使用情形，定期檢視系統效能、異常事件、適用性及應用效益，必要時採取調整、暫停或退場等處置，以落實 AI 全生命週期管理，確保 AI 於臨床場域之安全性、有效性及可信賴性。
- 三、另為掌握國內臨床 AI 之應用現況，本部已建置「全國臨床 AI 應用登錄平台」，逐步彙整醫療機構導入 AI 系統之基本資訊、應用目的、使用場域及治理情形，作為推動資訊透明、持續監測及後續政策規劃之參考。建議於報告相關段落適度納入上述推動情形，以完整呈現我國醫療 AI 治理機制。

參採情形：

第一點至第三點意見，錄供參考。

衛生福利部醫事司：

有關強化 AI 醫療隱私保護規範，宜對 AI 醫療的隱私保護建立完

整規範，例如個人資料去識別化的保護及加密處理、降低被識別風險、資料管理權限、跨院或跨機構的資料整合之建議，建議如下：基於 AI 發展日新月異，如何達到去識別化、加密處理、資料管理權限等方式，偏屬技術性質，此部分宜由數發部或其相關技術單位協助訂定技術性文件，以提供各目的事業主管機關及各業別使用。

參採情形：

本意見錄供參考。

衛生福利部食品藥物管理署：

- 一、並非所有醫療相關軟體都是醫療器材，《醫療器材管理法》對醫療器材有明確定義，醫用軟體是否屬於醫療器材，建議參考食品藥物管理署 111 年 9 月 15 日公告之「醫用軟體分類分級參考指引」。<http://www.fda.gov.tw/tc/siteListContent.aspx?sid=310&id=41636>。
- 二、有關資安部分，醫療器材查驗登記為上市前審查，本署已公告「適用於製造業者之醫療器材網路安全指引」供業者參採，涉及資料傳輸之產品，於查驗登記時要求業者提供網路安全評估。
- 三、國內尚未核准加入 AI 系統之達文西機器人用於 real-time 影像處理、操作輔助、手術自動化等功能。報告第 4 頁醫療工具開發一段提及「AI 也促進新一代醫用…即在操控輔助、實時影像處理、手術自動化與手術影像輔助等模組加入 AI 系統」，建議修改為「AI 也促進新一代醫用…即在操控輔助、實時影像處理、手術自動化與手術影像輔助等模組『研擬』加入 AI 系統」。
- 四、報告第 13 頁所載「美國 FDA 將醫療 AI 作為醫療器材軟體進行監管」，建議修正為「美國 FDA 負責醫療器材軟體的監管」。

參採情形：

- 一、第一點及第二點意見，錄供參考。
- 二、第三點及第四點意見，均已參採修正相關內容。

趙研究員俊祥：

- 一、報告探討了歐盟 AIA 將醫療 AI 納入「高風險」並有嚴格的全生命週期監管。但在我國現制下，衛福部食藥署本就透過《醫療器材管理法》及 PCCP（預定變更控制計畫）對軟體醫療器材（SaMD）進行嚴格查驗登記。報告雖點出我國缺乏明確的「高風險 AI 認定程序」，但未進一步釐清「經食藥署核准的 AI 醫療器材」是否即等同於《人工智慧基本法》所指的高風險 AI？二者在主管機關（食藥署 vs. 衛福部資訊處/各司處）、審查標準及法律責任上有整合的必要，否則容易形成多頭馬車或雙重合規負擔。建議衛福部應主動對接數發部的「人工智慧風險分類框架」，明確公告「食藥署列管之 SaMD/AI 醫療器材」與「基本法高風險 AI」的對應對照表。對於已經過嚴格二級/三級醫療器材審查的 AI 系統，其上市前審查應可直接視為符合高風險 AI 的部分合規要求，避免業者面臨衛福部醫材法規與數發部 AI 管理法規的雙重審查。
- 二、報告提及我國《人工智慧基本法》第 18 條給予各主管機關 2 年內完成法規調適，並以數發部於 115 年 7 月 7 日發布的「人工智慧風險分類框架」為據。然而，醫療領域具高度的「生命身體法益」專業性，若僅依行政指導性質的「指引」（如衛福部的生成式 AI 指引）來規範高風險醫療 AI，在行政法學上恐有違反法律保留原則之虞。若涉及限制人民權利或加重醫療機構、醫師之法定責任與罰則，仍需有明確的法律授權依據（如修訂《醫療法》

或《醫療器材管理法》)，單靠行政指引或行政規則，在司法訴訟或實務執行上面臨強制力不足的問題。建議主管機關不宜僅停留在發布行政指導性質的「指引」。應推動將《人工智慧基本法》關於高風險 AI 的義務，具體落實於《醫療法》或《醫療器材管理法》中，明確授權主管機關訂定醫療 AI 的驗證、資安、隱私及臨床試驗規範，以符合法律保留原則並使其具有強制力。

三、報告引用學者見解提及醫師使用合法的 AI 醫材時應受法律保護，但同時又強調醫師負「最終責任」。在民刑事責任實務（如過失傷害或醫療過失致死罪）中，我國刑法與民事侵權行為的過失判斷標準仍以「臨床醫療水準（Standard of Care）」為主。若 AI 系統已取得國家許可且符合臨床指引，但醫師基於專業自主「不採用」或「盲目採用」而發生醫療事故，現行實務法理對於「符合國家級認證之 AI 診斷結果」是否能阻卻醫師過失，缺乏明確的免責或舉證責任轉移設計。若一律將最終責任推給醫師，恐導致醫師產生極大的「防衛性醫療」心態，反而阻礙醫療 AI 的導入。為解決醫師的責任恐慌並避免防衛性醫療，建議未來在研議救濟、補償或保險機制時，可參考歐盟 PLD 的立法精神，針對「使用已取得我國合法許可且遵循 PCCP 變更控制之高風險 AI 醫材」的醫師，於法規中明定其在遵循特定臨床指引情況下的合理信賴保護或過失推定減輕機制，並透過強制性的「醫療 AI 專業責任險」來分攤風險，而非單純將責任加諸於個人醫師或醫院。

參採情形：

第一點至第三點意見，供主管機關納入後續制度研議參考。

李副研究員志遠：

- 一、本報告就人工智慧應用於醫療領域所涉及之風險分級、責任歸屬、隱私保護及心理健康應用等重要議題進行研析，並參考世界衛生組織、歐盟及美國之治理經驗，提出相應之法制與政策建議，研究內容完整且具前瞻性。尤其報告兼顧醫療科技創新、病人安全與權益保障，所提建立風險管理規範及完善責任與救濟機制等建議，方向妥適，值得主管機關納入未來法規調適及政策規劃之參考。
- 二、本報告提及我國醫療 AI 風險分級規範尚不完備，以及高風險應用認定標準未臻明確等問題。未來主管機關宜依《人工智慧基本法》及數發部所定之 AI 風險分類框架，研訂醫療 AI 風險分類及管理規範，明定高風險醫療 AI 之認定標準、審查程序、在地驗證、人類監督、上市後監測、不良事件通報及退場機制，並釐清相關機關之權責分工。
- 三、本報告已探討醫療 AI 可能涉及開發者、醫療器材業者、醫療機構及醫事人員間之責任分配，並指出現行救濟、補償及保險機制仍有不足。未來主管機關宜建立醫療 AI 不良事件通報及責任追溯制度，要求業者與醫療機構妥善保存模型版本、系統更新、操作紀錄及人工覆核情形，並研議責任保險、業者財務擔保或特別補償機制，以兼顧病人權益、醫事人員合理信賴及醫療科技創新發展。

參採情形：

第一點至第三點意見，與本報告方向一致，相關建議供主管機關研議參考。

陳副研究員育靖：

- 一、報告第 2 頁，「……醫療機構所持有的資料，不僅具有高度敏感性與隱私性，更具有不可逆與不可替代的特性，一旦外洩不僅僅是侵犯隱私，更可能引發保險歧視、無法即時核保，甚至社會排除等長期後果。……」一節，首先，「不可逆」通常是指「無法恢復」之狀態（例如：資料外洩導致不可逆的損害等），此處指出醫療資料具有不可逆特性所指為何？請進一步說明。又倘醫療資料外洩，自可能引發嚴重問題，但此處特別指出引發保險歧視、無法即時核保等問題，似乎與資料外洩並非具有直接關聯性，亦非資料外洩所應關注之重點。AI 應用於醫療產生之歧視或偏見問題，可能非資料外洩，而是用以訓練之資料或演算法有所偏誤。因此，透過法律要求使用 AI 時，必須確保演算法不會對特定群體造成歧視或不公平之結果（如《人工智慧基本法》第 4 條第 6 款規定），爰請再酌。
- 二、報告第 9 頁，針對歐盟法規部分，第一段之《人工智慧責任指令》（AI Liability Directive）與（二）修訂版產品責任指令一段所提到的《AI 責任指令》應屬同一指令，建議寫法一致，或於第一段註明（以下簡稱《AI 責任指令》）至於英文名稱則無須重複臚列。
- 三、報告第 18 頁，「肆、我國 AI 應用於醫療領域之相關規範」之「一、醫療器材管理法」，因該段多數係介紹相關指引而非《醫療器材管理法》，建議標題調整為「醫療器材管理相關法規」，以符實際。

四、報告第 22 頁，「……為因應上述風險，衛福部進一步提出醫療機構導入生成式 AI 的治理原則與管理措施，並提出 9 項要點協助機構按生成式 AI 導入生命週期規劃與執行：（一）「導入前評估階段」……」一節，指出衛福部提出 9 項要點協助機構規劃執行，惟該段以下係分為 3 個階段，並未看到 9 項要點，倘若係融入於 3 階段中論述，建議調整該段表達方式。

五、報告第 22 頁，（二）「導入與整合階段」一節，列出許多英文簡稱，如（EMR）、（HIS）、（PACS）與（LLMs）等，但皆未列完整英文名稱，建議補充之。

參採情形：

第一點至第五點意見，均已參採修正相關內容。

散會：下午 3 時 50 分