

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

張冠群*

壹、緒論：演算法掀起的醫療行為 注意義務轉型

醫療實務正經歷一場結構性轉型，其規模與潛在影響力宛如當年細菌致病理論的提出。人類正在見證一個時代的過渡：從單純依賴人類判斷並輔以靜態工具診斷與實施醫療行為的時代，進入「演算法醫療」(Algorithmic Medicine)時代，決策權力正日益倚賴並讓渡給人工智慧系統¹。這些系統，特別是基於機器學習 (Machine Learning) 和生成式預訓練變換模型 (GPT) 的系統，具備自主性、不透明性和可塑性，正悄然挑戰著侵權行為法 (Tort Law) 和監督管理的基礎原則²。

在此一不可逆的趨勢下，本文欲提出的核心問題為：AI整合進醫療臨床實行行為，不論診斷或治療，創造了一個「責任缺口」，此缺口乃一個法律不確定性的地帶，傳統侵

權法原則未能適當地分配自主系統造成損害的責任歸責與賠償。故，當演算法從「決策支援」演變為「決策制定」時，傳統的侵權行為及損害賠償法面臨責任主體與歸責對象的危機，例如：診斷演算法究竟是產品還是服務？倚賴演算法進行診斷的醫師是「專業中間人」(Learned Intermediary) 抑或是單純的資料輸入員？而當演算法的「黑盒子」失靈導致失療失敗，病患權利受侵害時，醫師、醫院或系統開發商，孰應負損害賠償責任？而未將此風險納入定價的醫師專業責任險的保險公司需否理賠？

在重點發展及巨額資金挹注下，全球醫療AI市場預計將達到數千億美元，然而支撐此一市場的法律基礎設似乎尚未跟上技術的快速發展。在歐盟，政策制定者採取了全面的預防性立法改革，明確將軟體重新定義為產品並取消責任上限³。相比之下，美國採取了碎片化、部門化的路徑，依賴聯邦FDA法規

* 本文作者係中信金融管理學院教授兼保險金融研究中心執行長

註1：W. Nicholson Price II, *Clinicians in the Loop of Medical AI*, 74 EMORY L. J. 1265 (2025).

註2：Sara Gerke & David A. Simon, *New Case Law and Liability Risks for Manufacturers of Medical AI*, 388 SCIENCE 1138 (2025).

註3：Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, 2024 O.J. (L 2853).

(常透過優先權原則保護製造商) 以及各州不斷演變的法規拼湊而成⁴。

本文分為六個部分。第二部分探討醫療AI的技術分類及AI醫療責任歸屬的難題。第三部分分析新興的歐洲架構，特別是2025年撤回《AI責任指令》後轉而依賴修訂版《產品責任指令》的影響。第四部分檢視美國的法律圖像，聚焦於FDA優先權、代表性的州立法及指標性判例法與使用AI進行醫療程序之醫療責任可能變化。第五部分探討AI醫療應用對責任保險市場之衝擊，並分析「沈默的AI」(Silent AI)風險與新的除外條款。第六部分深入探討責任保險對於AI醫療關於責任歸屬的新興法理爭論與責任區塊的漂移於實務面之回應。最後，第七部分則綜合前六部分之討論，提出關於AI醫療責任歸責制度之建議並評估其他補償模式之可行性。

貳、人工智能在醫療領域的用及衍生的責任歸屬難題

一、AI在醫療領域之應用

人工智能 (Artificial Intelligence, AI) 在醫療領域的應用日益廣泛，主要涵蓋以下方面：

(一) 診斷支援系統 (Clinical Decision Support Systems, CDSS)：利用機器學習模型分析影像、基因資料或電子病歷，提供診斷建議⁵。

(二) 手術輔助與機器人手術：AI輔助的手術系統可精準控制手術器械，減少醫療疏失風險⁶。

(三) 病歷管理與預測分析：AI可對大量醫療數據進行整理與風險預測，協助醫師做出決策⁷。

(四) 保險理賠自動化：AI模型可快速評估醫療費用合理性，決定理賠與否⁸。

成問題者，這些應用雖帶來效率與精準度的提升，但同時產生「黑箱問題」：醫師及患者往往無法完全理解AI系統的決策邏輯，增加法律責任的風險與不確定性⁹。

二、AI於醫療應用的責任歸屬難題

欲徹底解構人工智能於醫療領域應用的法律責任歸責鍊的斷裂，首先必須理解技術的轉變。傳統醫療器材（如手術刀、心律調節器）是確定性的；其故障模式是機械性且可預測的。然而，AI系統引入了三個干擾傳統責任分析的新特徵：不透明性 (Opacity)、自主性 (Autonomy) 與可塑性 (Plasticity)。

註4：See Utah S.B. 226, 2025 Gen. Sess. (Utah 2025) (amending the Utah Artificial Intelligence Policy Act).

註5：Sherry L. Willis & Robert S. Chen, *Artificial Intelligence in Healthcare: Applications and Legal Challenges*, 45 J. Health L. & Pol'y 123, 130-35 (2023).

註6：Ibid. at 136.

註7：Benjamin R. Jacobson, *Machine Learning in Clinical Practice: Risk and Liability*, 12 Yale J. Health Pol'y, L. & Ethics 89, 92-95 (2022).

註8：Ibid. at 98.

註9：Virginia Dignum, *Responsible Artificial Intelligence: Designing AI for Human Values* 67-70 (2020).

(一) 自主性光譜與「黑盒子」不透明性

醫療AI運作於自主性光譜上，光譜底端是臨床決策支援（Clinical Decision Support）系統，其利用固定規則標記藥物交互作用，而光譜高端則是利用「黑盒子」機器學習的自主診斷系統（Autonomous diagnostic systems）。不同於基於規則的AI，機器學習系統從海量數據中學習的模式，發展出人類往往無法理解的數學上相關性¹⁰。然而，正音無法理解，也創造了不透明。這種不透明性切斷了侵權行為法所需的因果關係鏈。在過失侵權訴訟中，原告必須舉證證明被告的侵害行為「如何」導致傷害，亦即證明被告之行為與原告損害間之因果關係。而如果「侵權原因」是神經網絡層中一個人類無法解釋的權重或變數錯誤，原告便無法盡到傳統侵權行為法上的舉證責任¹¹。這無異創造了一個責任的真空，製造商可藉此辯稱該錯誤是不可預見的統計異常，而非設計瑕疵。

(二) 可塑性與「特修斯之船」（Ship of Theseus）¹²問題

傳統監理的假設設備是「鎖定」狀態（Locked Device）。然而，AI系統通常是具適應性（adaptive）的，會隨著攝入真實世界數據而不斷更新內部模型¹³。這種可塑性創造了「特修斯之船」（Ship of Theseus）的理

論：在什麼時間點，一次更新會使該AI成為需要重新認證的「新」設備？

例如倘若演算法因病患人口結構改變而發生「模型漂移」（Model Drift）並隨後因錯誤的診斷造成損害，這是原始設計的失敗（製造商責任）還是監測的失敗（醫療提供者責任）？美國FDA依賴「預定變更控制計畫」（Predetermined Change Control Plans）雖然正試圖對此動態技術施加監理，但當一個AI「演化」至缺陷狀態時的責任歸屬仍未有定論亦尚未驗證¹⁴。

參、歐盟法及其監理落地

歐盟致力於推動一個集中的、「橫向」立法計畫以使責任制度現代化。然而，2025年此一具指標性策略出現重大轉折，即《人工智慧責任指令》（AI Liability Directive）因分歧過大而暫時撤回。目前，歐盟的監理版圖目前包含三項與醫療AI相關的主要法規範工具。

一、醫療器材法規（MDR）與軟體醫療器材

首先，歐盟第2017/745號法規即醫療器材

註10：W. Nicholson Price II, *Black-Box Medicine*, 28 HARV. J.L. & TECH. 419 (2015).

註11：Andrew D. Selbst, *Negligence and AI's Human Users*, 100 B.U. L. REV. 1315 (2020).

註12：特修斯之船是一個哲學思想實驗，探討身分和變化的本質。這個悖論源自於希臘哲學家普魯塔克的思考，它提出了一個問題：如果一個物體的所有部分都隨著時間的推移而被替換，它是否基本上保持不變。

註13：U.S. FOOD & DRUG ADMIN., Artificial Intelligence & Machine Learning (AI/ML)-Enabled Medical Devices (2024).

註14：See Sara Gerke et al., The Need for a System View to Regulate Artificial Intelligence/Machine Learning-Based Software as Medical Device, 3 NPJ DIGIT. MED. 53 (2020).

法規（EU Medical Device Regulation, 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, AI 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（Conformité Européenne）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AI SaMD製造商規劃持續臨床評估、風險管理及網路安全措施。承保過程中，保險公司通常要求提供合規證明¹⁵。

二、人工智慧法案（EU Artificial Intelligence Act）：作為責任前提的安全要求

《歐盟人工智慧法案》（2024年7月12日刊登於官方公報）是一項橫向立法，依風險對AI系統進行分類，並對「高風險」系統（可能包括許多臨床決策支援工具及特定SaMD）增加要求。AI法案在透明度、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了新的法令遵循義務¹⁶。關鍵條文為第14條強制規定高風險AI系統的設計必須能夠實現有效的真人監督（human oversight）¹⁷。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。

三、修訂版產品責任指令（Product Liability Directive, PLD）

隨著擬議的《AI責任指令》（AI Liability Directive）因政治分歧於2025年2月被撤回¹⁸，歐盟實際上透過修訂版《產品責任指令》將1985年關於瑕疵產品的指令現代化，將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」，解決了數十年的不確定性¹⁹。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，賠償請求權人無需證明開發者有過失。擴大了可請求賠償

註15：REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

註16：Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), O.J. L (July 12, 2024).

註17：Id. at Art. 14.

註18：European Commission, Withdrawal of Commission Proposals, 2025 O.J. (C 12) (Feb. 12, 2025).

註19：Directive (EU) 2024/2853, supra note 3 at Art. 4.

的損害範圍，延長了售後義務，並在原告面臨過度技術困難時創設了瑕疵與因果關係的推定²⁰，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了巨大的潛在法律風險²¹。另，傳統上，「開發風險抗辯」(Development Risk Defense) 允許製造商在證明流通時的科學知識水平無法發現缺陷的情況下免責。修訂版PLD針對AI大幅限縮了此抗辯。它規定，如果缺陷是由於缺乏必要的軟體更新，或者製造商保留了對軟體的控制權，則此抗辯不適用²²。再者，新版PLD採用瑕疵推定制度，其為解決「黑盒子」證據缺口，引入了可推翻的推定(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」造成了損害，法院可推定該產品存在缺陷²³。這有效地將舉證責任轉移給製造商，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。

肆、美國法：聯邦、州及判例法的多軌運作

與歐盟的集中式改革形成鮮明對比，美國透過聯邦法規與州普通法（Common Law）組

成的複雜架構來管理醫療AI責任。

一、FDA對醫療器材AI / ML的方法

食品藥物管理局(FDA)將醫療AI作為「醫療器材軟體」(SaMD)進行監管。器材的分類決定了製造商享有的責任與保護。

FDA採取者，為漸進式監理策略。早期FDA措施包括2019-2021年針對數位健康的重點指導，以及2021年*AI / ML-Based Software as a Medical Device Action Plan*，明確上市前期望並提出持續學習算法的監管方案。此後，FDA發布多份指引與草案指引(如預定變更控制計畫PCCP及「全產品生命周期」方法)，旨在兼顧適應性AI的安全性與效能要求。FDA將符合法定定義的SaMD被視為醫療器材，採用上市前核准(510(k)、De Novo、PMA)及上市後監測工具²⁴。

然與歐盟不同者，美國缺乏統一橫向之AI法規，監理仍為部門及機構主導。FDA框架雖已保留彈性，然對迭代更新、透明性要求及軟體變更是否需重新提出核准仍留有疑問²⁵。

二、侵權法原則：醫療過失、品責任與因果關係

在美國，傳統醫療過失要素—注意義務(duty of care)、義務違反(breach)、因果

註20：European Commission, Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive), COM (2022) 496 final (Sept. 28, 2022).

註21：Directive (EU) 2024/2853, supra note 3.

註22：Id. at Art. 10(2).

註23：Id. at Art. 9.

註24：FDA, Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan (2021) available at https://www.fda.gov/media/145022/download?utm_source=chatgpt.com.

註25：*Ibid.*

關係（causation）、損害（damage）——仍為臨床錯誤求償主要途徑。當AI影響臨床決策時，原告可針對醫師對錯誤AI建議的過失依賴或未適當覆核為理由提起侵權行為訴訟。另可針對製造商提出基於產品責任的損害賠償請求（設計瑕疵、未警告、製造缺陷）。然而，某些司法管轄區對軟體是否屬於「產品」仍存爭議，法院有時不將複雜軟體與實體商品同列為產品²⁶。

實證研究顯示，截至2020年中期，針對AI醫療過失的陪審團判決案例數量仍相對稀少，案例法缺乏增加法律不確定性，進而影響保險公司風險評估²⁷。

學說則認為，傳統上，專業中間人原則（Learned Intermediary Doctrine）主張，若製造商已向開立處方的醫師提供充分警告，則製造商可免除對病患的直接責任²⁸。此原則預設醫師能夠理解並評估風險。而在「黑盒子」AI的背景下，此原則必然失效。如果醫師無法理解神經網絡為何得出特定診斷，醫師便無法充當「專業」的中間人²⁹。近期的訴訟，如*Sampson v. HeartWise Health Systems* (2023)，顯示法院越來越懷疑是否

應允許將醫師作為不透明演算法失靈的責任擋箭牌³⁰。

三、州立法回應：安全港的興起

由於聯邦行動緩慢，各州已開始制定自己的AI法規。代表性之立法如下：

(一) 猶他州：「安全港」（Safe Harbor）模式

2025年修訂的《猶他州人工智慧政策法案》（Utah Artificial Intelligence Policy Act）建立了一個監理安全港。該法案規定，如果在受監管的職業（包括醫療）中清楚揭露生成式AI的使用，則該使用者不會因欺詐性行為而受到公權力機關強制措施³¹。這反映了一種支持創新的策略，以透明度交換責任豁免。

(二) 喬治亞州：「人機迴圈」強制令（Human in the Loop Mandate）

喬治亞州的SB 473禁止僅基於AI結果做出醫療決策。它強制要求所有AI驅動的決策必須經過「有意義的真人審查」（meaningful human review）³²。此法規試圖將「人機迴圈」（Human-in-the-Loop）法制化為責任防護

註26：Georgegerke Maliha et. al, Artificial Intelligence and Liability in Medicine: Balancing Safety and Innovation, 99(3) *The Milbank Quarterly* 629-647 (2021).

註27：Gennie Mansi & Mark Riedl, Implications of Current Litigation on the Design of AI Systems for Healthcare Delivery (2025) available at <https://arxiv.org/pdf/2507.15981v1.pdf>.

註28：RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 6(d) (AM. LAW INST. 1998).

註29：W. Nicholson Price II & I. Glenn Cohen, Locating Liability for Medical AI, 73 DEPAUL L. REV. 339 (2024).

註30：Sampson v. HeartWise Health Sys. Corp., No. 22-cv-1234 (E.D. Pa. 2023).

註31：Utah Code Ann. § 13-2-12 (West 2025).

註32：S.B. 473, 157th Gen. Assemb., Reg. Sess. (Ga. 2024).

網，但也可能使那些「橡皮圖章」式批准AI輸出的醫師面臨懲戒及侵權責任。

四、代表性判例法及分析

雖然臨床決策中使用先進AI尚屬新興現象，但現有美國醫療技術訴訟已為醫師、醫院與技術開發商之間責任分配建立了法理基礎。法院已展現出檢驗臨床醫師與製造商之間義務及資訊揭露說明義務有無之趨勢，尤其在醫師將軟體或機器人系統納入治療流程時更是如此。

(一) AI輔助醫療中的產品責任與醫療人員責任之分配

現代醫療過失原則關鍵在於損害究來自醫師的疏失，抑或軟硬體技術本身的缺陷。

院認為，先進醫療系統通常呈現黑盒特性，操作需要專門知識；製造商可能對操作訓練及風險溝通承擔注意義務。在*Taylor v. Intuitive Surgical, Inc.* 一案中，雖然本案發生於深度學習AI之前，但於查探現代司法對此認識上仍屬開先河之案例，甚具參考價值。

本案中，華盛頓州最高法院認為，機器人手術平台製造商對醫院（作為機構購買者）而非個別外科醫師，承擔充分指導與警告的義務。製造商責任因此超越傳統產品分銷概念，反映了現代臨床技術的制度性與系統性特質³³。

*Taylor*案的建立的判斷原則，拒絕了「只要醫師誤用即可免責製造商」的簡化論點。法院審查重點在於：產品是否缺乏足夠警語或訓練程序，而此一邏輯可直接套用於AI診斷

演算法。若AI誤判之風險、未能適當從更新資料集學習之風險，或未能建議次優治療方案等等，若製造商對該些風險提供的警告不足或具誤導性，其仍有責任，故應負賠償責任者，可能不僅限於有醫療過失之醫事人員。

(二) 先占原則（Preemption Doctrine）與器材核准之問題

在*Riegel v. Medtronic, Inc.* 案中，美國最高法院認為，若醫療器材已通過FDA上市前核准（Premarket Approval, PMA），州法律下對製造商的責任主張將受到先占限制，因PMA過程涉及嚴格的監理審查，相當於對產品安全性及標示標準的核准，因此優先於州侵權法規範適用³⁴。

此判例為原告提出AI驅動設備相關訴訟設下重大程序門檻。若未來AI診斷設備或手術系統獲得PMA批准，設計瑕疵或警告不足之侵權行為責任均可能被排除，此將促使原告究責轉向：(1)質疑醫師對AI工具的使用；(2)主張醫療行為實施過程中的疏失而非設計缺陷；或(3)提出聯邦訴訟，例如對FDA提出詐欺之訴（但受*Buckman*案限制甚嚴）。

*Riegel*案產生的法理缺陷為：對自動適應、持續學習AI系統所產生的法理不確定性。蓋PMA核准通常針對靜態產品配置，但許多AI診斷系統會隨新臨床資料更新而動態調整，而倘AI運行狀態顯著偏離起初核准之基礎模型，法院可能認為PMA保護不再適用，因實際運作之模型版本已與核准版本不符。此問題在判判例法及監理法規解釋中仍屬待釐清問題。

註33：*Taylor v. Intuitive Surgical, Inc.*, 389 P.3d 517, 528-29 (Wash. 2017).

註34：*Riegel v. Medtronic, Inc.*, 552 U.S. 312, 330 (2008).

(三) 綜和評析AI參與醫療決策時的責任分配

綜合Taylor與Riegel案，可觀察到兩個對立的趨勢：Taylor擴大複雜醫療機械製造商潛在責任，承認其警告與訓練義務；然Riegel則透過聯邦先占限制州侵權索賠，收縮製造商責任。

對AI驅動系統而言，責任分配有三構面：(1)醫師：專業過失；(2)醫院或醫療機構：未充分實施控管、訓練或監督AI使用；(3)AI開發者或製造商：警告不足、演算法偏差或訓練資料缺陷。此三構面推演出的可能訴訟結果為：若法院沿Taylor案判斷，醫院可能成為AI輔助醫療傷害訴訟中的主要被告，因其負責培訓與部署，而製造商在AI工具獲得PMA核准且相對靜態時，可能部分免責（受Riegel案保護）；另方面，若AI系統動態更新、持續自我學習，原告可主張PMA先占不適用，因實際部署演算法超出FDA核准配置，此際，法院可能要求明確劃分監督角色，判定醫師是否應主動覆核AI建議（human-in-the-loop義務），或可合理依賴算法決策。

五、AI運用於醫療對責任保險市場之變革

一、核保、承保險種與除外條款

承保醫療糾紛與網路／產品責任的保險公司面臨AI帶來的新型風險³⁵：

(一) 醫療過失責任之被保險人

醫療糾紛保險公司將被要求承保臨床醫師依賴AI工具的索賠。核保必須考量：醫療提供者是否採用改變注意義務標準的工具、供應商在契約上如何分配責任（賠償條款），以及醫院如何監督AI的使用。

(二) 科技錯誤與遺漏（Tech E&O）

供應商（SaMD、EHR與AI演算法開發者）通常會購買E&O與產品責任險。這些險種的核保人員將日益針對演算法風險、軟體更新風險、數據漂移（data-drift）及模型重新訓練風險進行定價。歐盟的PLD延長了售後責任並在複雜案件中推定因果關係，相較於美國，顯著增加了供應商在歐洲的風險。

(三) 網路與隱私保險

含醫療AI在內的許多AI系統依賴大數據與雲端平台；資料外洩將觸發資安保險的保險事故。隱私損害與數據遺失在修訂版PLD下屬於新認定的損害，且在歐盟可能是可請求理賠的，這將影響資安保險的承保風險內容。

(四) 除外條款與次限額

保險公司可能會在契約條款中加入針對「已知未經驗證AI系統」的除外條款，或增加針對演算法索賠的次限額，或要求穩健的供應商驗證與可解釋性實務作為核保條件。

二、保費、承保量能與再保險

索賠頻率的上升與演算法失靈的系統性本質，如一個廣泛部署模型的錯誤可能同時觸發大量理賠請求）引發了承保量能（Capacity）的擔憂。再保險公司與資本市場

註35： Pinsent Masons, Revised EU Product Liability Regime Expands to AI Software Providers, <https://www.pinsentmasons.com/out-law/analysis/revised-eu-product-liability-regime-expands-ai-software-providers> (last visited Nov. 27 2025).

對累積風險（Aggregation Risk）非常敏感；若多家醫院使用相同的AI系統，可保損失可能具相關性，推高再保險成本或導致再保險公司限制承保量能。歐盟的監管方案（擴大責任與售後責任）增加了供應商潛在的累積風險，這可能轉化為供應商面臨更高的保費或更少的保險選擇，並可能導致與其簽約的醫療提供者面臨更高的醫療糾紛保費³⁶。

三、風險緩減條款與契約分配

保險公司與大型醫療體系將日益使用契約款之設計方式（如加入賠償條款、免責條款、供應商保固及穩健的服務層級協議）在提供者與供應商之間分配風險。然而，此類契約分配可能受到侵權法及衡平法原則例如顯失公平、對非契約當事人的義務及監督義務（例如MDR / AI法案對使用者與主管機關的義務）的限制。保險公司承保時將要求提供以下證據：(i)AI的穩健驗證 / 臨床評估；(ii)監控與上市後監督；(iii)可解釋性功能；及(iv)清晰的軟體更新與治理³⁷。

四、「沈默的AI」現象

保險公司面臨「沈默的AI」（Silent AI）風險—即一般責任保單中未定價涵蓋演算法失

靈的潛在風險³⁸。例如，若醫院的AI驅動空調系統因「幻覺」（Hallucination）而故障導致疫苗損毀，這是一般財產損失還是網路保險承保之損失？再保險公司正施壓原保險人引入特定除外條款，例如ISO批單CG 40 47，明確排除源自生成式AI的責任³⁹。

五、演算法績效保險

為填補保障缺口，慕尼黑再保（Munich Re）等公司推出了針對特定的AI保險產品（如aiSure）。這些保單承保績效保證。如果AI系統未能達到承諾的準確率，保險公司將賠償使用者的損失⁴⁰。這將AI風險從侵權問題（是否有過失？）轉移為保固問題（是否達到其應有的效能？）。

陸、AI醫療衍生之責任保險法理爭論及再設計

一、醫師責任保險

(一) 變動中的注意義務標準

醫療過失保險於二十世紀初在美國興起，因醫師面臨日益增加的過失訴訟⁴¹。醫師責任保險關於保險事故發生，係於醫療過失

註36：*Ibid.*

註37：FDA, Artificial Intelligence-Enabled Medical Devices,

<https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-enabled-medical-devices> (last visited Nov. 27 2025).

註38：See SWISS RE INST., AI Risk: The Silent Cyber of the Future? (2024).

註39：INS. SERVS. OFFICE, INC., Commercial General Liability Endorsement CG 40 47: Exclusion-Generative Artificial Intelligence (2024).

註40：Munich Re Launches aiSure to Back Performance of AI Solutions, MUNICH RE (2023).

註41：Kenneth S. Abraham, Liability Insurance and Tort Law: An Introduction, 12 Conn. Ins. L.J. 1 (2005).

(Malpractice) 侵權行為責任之成立。自二十世紀起，美國法建立之標準為：醫師未達到專業標準之照護義務⁴²，亦即醫療過失有無之判斷乃要求醫師照護義務履行行為是否符合「理性醫師」標準⁴³。對此一責任風險，醫師通常以索賠基礎（claims-made）型醫療過失責任保險移轉其責任風險⁴⁴，醫院亦同時投保機構責任保險⁴⁵。此一傳統侵權行為責任及對應之責任保險運作之基本前提為：醫師為主要決策者、醫師控制診斷與治療過程且醫師之專業判斷為醫療損害之直接原因。

惟當醫師依賴AI醫療輔助系統時，此一前提便產生結構性崩解。例如，放射科醫師使用AI產製之異常偵測影像建議以判斷腫瘤是否存在時，其依賴或拒絕AI建議的行為即成因果鏈的一部分。若AI因訓練資料偏差而對某特定族群群體做出系統性的誤判—例如在某亞裔族群中系統性產出錯誤的負面偏誤（false negatives），則責任應歸於醫師、醫院、軟體供應商、資料提供者、監理者或以上皆是？

此一情形直接衝擊醫師責任中「理性醫師」（Reasonable Physician）標準。在人工智能情境下，法院可能將「合理使用人工智能」納入此標準。申言之，醫師若依賴有瑕疵之AI（自動化偏差），仍可能需承擔責

任。例如放射科醫師依賴AI而漏診腫瘤。責任究竟在醫師（不合理倚賴）或製造商（演算法缺陷）？這直接關係病患遭受的損害是否屬醫師責任保險的承保範圍，亦為影響病患應向誰求償之關鍵。反之，隨著AI系統在放射學等領域展現出超人類的準確性，理性醫師判斷標準將不可避免地轉向「未使用AI導致誤診之責任」⁴⁶亦即，當AI之診斷以準確至超越人類時，未能諮詢經過驗證的AI診斷工具亦可能構成醫療過失。此一現象讓醫師陷入危險的雙重束縛：如果使用AI而它失敗了，需負責；如果不使用AI而錯過了診斷，也可能需負責⁴⁷。

（二）責任保險之設計改革建議

本文認為，在醫療程序愈來愈倚賴AI的趨勢下，關於各主體責任分配，可區分為下列三面向：

1. **使用過失（Use-Fault）** — 醫師之錯誤
依賴或不當排除；
2. **設計過失（Design-Fault）** — 開發者之演算法失準或資料偏誤；
3. **整合過失（Integration-Fault）** — 醫療機構未建立風控與監督機制。

針對上開醫師過失責任認定標準法理在AI應用之衝擊及上開之責任分類，本文建議傳統醫師責任險保單應增列下列承保範圍：(1)

註42：Prosser & Keeton on the Law of Torts § 32 at 185 (5th ed. 1984).

註43：Hall v. Hilbun, 466 So. 2d 856 (Miss. 1985).

註44：Tom Baker, *Medical Malpractice and the Insurance Underwriting Cycle*, 54 DePaul L. Rev. 393 (2005).

註45：Kenneth S. Abraham & Paul C. Weiler, *Enterprise Medical Liability and the Evolution of the American Health Care System*, 108 Harv. L. Rev. 381 (1994).

註46：Michelle M. Mello & Neel Guha, *Understanding Liability Risk from Using Health Care Artificial Intelligence Tools*, 390 NEW ENG. J. MED. 271 (2024).

註47：*Id.* at 273.

對AI輸出之合理依賴錯誤之保障；(2)倘損害之發生係因演算法解釋爭議，醫師個人所支出抗辯費用；(3)若醫師已進行合理審查與紀錄，則可建立責任安全港（safe harbor），其重要性在於：若醫師已遵循醫療AI使用規範並紀錄判斷理由，責任應向其他主體移轉，此際保險公司對被保險醫師應有防禦與抗辯義務。

二、產品責任保險

(一) AI醫療下產品責任面臨之歸責困境

傳統上，有缺陷之醫療器材適用產品責任—製造商對產品缺陷負嚴格責任⁴⁸。然而AI醫療系統通常具混合性：其核心可能是持續自我更新之演算法，而更新透過雲端結構並吸收新資料。不同於心律調節器或導管，AI醫療產品並非靜態固定。在產品責任成立極端依賴於產品於銷售時可被測試與驗證之性質前提下⁴⁹，因AI系統接受持續訓練，會更新其模型參數，導致醫療事件發生時之版本可能與初始核准版本不同而產生**時間性模型漂移問題**（temporal shifting-model problem），此一動態學習模組系統使品瑕疵分析更為困難，尤其AI部署後持續演化，難以界定銷售時之「瑕疵」。

另，AI究竟屬於產品或服務，於美國法律上亦乏定論。除非如歐盟《產品責任指令》已明確將軟體納入範疇⁵⁰，否則AI醫療軟體在

法律上是否構成「產品」可適用嚴格責任，或其僅為資訊服務，縱然美國《侵權法重述（第三版）》對「產品」已採廣義定義，解釋上可含括軟體⁵¹，但部分法院仍視軟體為服務。

(二) 責任保險之設計改革建議

本文建議，財產保險業針對AI產品的特殊情形，可開發提供專門針對AI開發者的產品責任保單。此一專門產品責任保險於醫療領域，可透過監理法規，採強制投保，其承保範圍應至少包括以下面向：

1. 開發者責任：

包括因演算法偏誤損害、AI產生之錯謬臨床建議、版本更新風險及因網路攻擊導致之資料扭曲之風險。

2. 雲端更新與追溯責任：

當AI模型透過雲端自動更新，而更新版本引發醫療事故時，配合責任釐清，被保險人需透過法規被課與歷史版本紀錄義務、同意模型取證工具（forensic model tracing），如此才有可能以保險轉嫁演算法演進過程瑕疵責任覆蓋。

柒、結論與建議：重新設計責任及保險層保範圍

人工智慧在醫療領域的應用，使傳統「醫師—病患」二元關係轉向「醫師—AI系統

註48：Restatement (Third) of Torts: Products Liability § 1 (1998).

註49：George W. Conk, *Punctuated Equilibrium: Why the Products Liability Restatement Should Be Revised*, 26 Yale J. on Reg. 215 (2009).

註50：Council Directive 85/374/EEC, as amended 2024 (EU Product Liability Directive).

註51：Restatement (Third) of Torts: Products Liability § 19 (Am. L. Inst. 1998).

—病患」的三元關係。誠如本文分析，AI的診斷支援、手術輔助與風險預測功能雖顯著提升了醫療效率，但其伴隨的「黑盒子」不透明性、自主性與可塑性，已對傳統侵權行為法與產品責任法的歸責基礎造成劇烈衝擊。

目前全球監理趨勢呈現「歐盟集中式」與「美國分散式」的雙軌發展。歐盟透過新版《產品責任指令》（PLD）與《人工智慧法案》（AI Act），傾向透過立法將軟體明確定義為產品，並引入過失推定與因果關係推定，以此解決原告在面對複雜演算法時的舉證困境，體現了保護消費者與病患權益的價值取向。相對地，美國則維持以FDA上市前核准（PMA）結合州法侵權訴訟的體制，雖保有創新彈性，但Taylor案與Riegel案的歧異顯示出司法實務在「先占原則」與「警告義務」間的擺盪，導致醫療提供者與技術開發商面臨高度的法律不確定性。

無論歐盟或美國法制，可確定者為：傳統侵權法已無法解決醫師責任與AI醫療產品間產生的「責任缺口」，結構性改革勢在必行。本文提供下列面向之改革建議以供決策者思考：

一、法律層面

確立軟體產品屬性與減輕舉證責任我國或未來立法論上，應參考歐盟修訂版PLD之精神，明確將醫療AI軟體納入「產品」之定義範疇，以適用嚴格責任，避免因「服務」或「產品」之定性爭議而使受害者求償無門。

此外，針對具高度技術複雜性之「黑盒子」AI系統，應適度引入舉證責任倒置或因果關係推定原則。若原告能證明產品運作異常且與損害間具有統計上之蓋然性，即應推定因果關係存在，改由掌握數據與演算法解釋權的製造商負舉證責任，以平衡醫病雙方之武器不對等⁵²。

二、責任保險與補償制度

推動「分層負責」的強制責任保險與新險種。鑑於傳統醫師責任險與產品責任險的邊界日益模糊，保險市場應針對AI醫療特徵進行結構性改革。本文建議採納前述「三面向責任」架構進行保單設計：(1)針對醫師：責任險應擴大承保對AI建議的「合理信賴」風險，並建立安全港條款，若醫師已履行人機迴圈（Human-in-the-Loop）之監督義務，應由保險機制承擔防禦成本；(2)針對開發商：應強制投保「演算法績效保險」或專屬產品責任險，承保範圍需涵蓋模型漂移、數據偏誤及軟體更新失敗所致之損害；(3)針對醫療機構：應強化資安與系統整合之承保範圍，以應對沈默的AI（Silent AI）風險。

上開三責任面向，又可以不同模式進行整合。本文建議可行之整合方向包括：

(一) 將責任從個別醫師轉移至醫院系統

(企業責任) ——醫院作為成熟的購買者，更有能力審查AI供應商、賠償醫師並吸收「系統性事故」的成本。這將責任與控制權對齊，可簡化受損害

註52：See European Commission, AI Liability Directive, supra note 16 (proposing rebuttable presumption of causality).

病患之求償與訴訟程序⁵³。

- (二) 有論者倡議，比照美國管理核能責任的《普萊斯—安德森法案》(Price-Anderson Act) 建立聯邦責任計畫。在此模式下，AI開發者需購買第一層保險，而第二層由產業資金池支付系統性與災難性之損害⁵⁴。這能防止導致破產的大規模侵權訴訟，同時確保受害者獲得賠償。
- (三) 更激進的方案為：模仿美國國家疫苗傷害賠償計畫(National Vaccine Injury Compensation Program, VICP) 的無過失補償機制⁵⁵。由認證醫療AI造成的傷害將移出侵權系統，由行政法庭裁決。這消除了在黑盒子演算法中證明「過失」的不可能負擔，承認部分演算法錯誤是創新過程中不可避免的統計副產品。

三、臨床治理

落實實質性的「人機迴圈」與動態監測。為避免責任轉嫁僅流於形式，醫療機構應建立嚴格的AI使用指引。醫師在使用AI輔助決策時，不應僅作為橡皮圖章，而須保留最終裁量權並記錄決策理由，以落實前開喬治亞州立法所強調的「有意義的真人審查」(Meaningful Human Review)。同時，製造商應配合FDA的「全產品生命週期」監理概念，建立上市後持續監測機制，確保演算法在真實世界數據下的穩定性，解決「特修斯之船」帶來的歸責斷裂問題。

總結而言，醫療AI的法律責任不應僅是「誰該賠償」的零和遊戲，而應透過法律明確化、保險商品創新與臨床治理的升級，建立一個能兼顧病患安全與技術創新的永續生態系。

註53：Price & Cohen, *supra* note 29, at 350.

註54：Price-Anderson Act, 42 U.S.C. § 2210 (2024).

註55：National Childhood Vaccine Injury Act of 1986, 42 U.S.C. §§ 300aa-10 to 34 (2024).