2026 理律盃校際法律系所學生模擬法庭辯論賽賽題

醫療 AI 系統責任之相關議題

1. 恆永健康診所（下稱「恆永診所」）是台灣具有相當規模之知名私人獨資健檢診所，負責人為甄恆永，專攻癌症篩檢及健康檢查等服務；經營模式包括培養長期客戶，與之簽署長期健檢方案。在醫事人員短缺、人工智慧技術蓬勃發展，及醫療器材軟體之應用日益提升的環境下，恆永診所標榜引進 AI 先進科技為客戶提供各類健檢套裝及方案服務，並另配合醫院提供 CT、磁振造影與正子電腦斷層等高階檢查。

2. 智醫核心科技股份有限公司（下稱「智醫核心」）為一新創的 AI 軟體開發公司，宣稱其旗艦產品「時真 AI 系統」能透過生成式 AI 模型與影像辨識技術，協助評估胸部 X 光影像，並進行肺癌風險預測與臨床輔助判斷，及快速自動輸出判讀結果與報告，以提供醫師後續進行肺癌診斷及篩選。另外，智醫核心具有製造、銷售醫療器材及醫療器材軟體的許可執照。

3. 在 2025 年初，甄恆永獲悉時真 AI 系統已完成階段測試，並正在申請醫療器材許可證查驗登記的階段，預定在取得醫療器材許可證後，約在第四季可完成相關準備工作，全面上市。由於所內醫事人員短缺，甄恆永在業界朋友引介下積極與智醫核心磋商，擬在其取得醫療器材許可證後儘速安裝並上線使用該系統，以緩解人員壓力。2025 年 4 月初，智醫核心就時真 AI 系統取得醫療器材許可證，隨後恆永診所於 2025 年 4 月 21 日與智醫核心簽訂「AI 輔助診斷系統採購與授權合約」（附件 1；下稱「系爭合約」），成為第一家使用時真 AI 系統的醫事機構。雙方具體合作方式為由智醫核心提供時真 AI 系統，安裝於恆永診所的伺服器中，恆永診所給予智醫核心存取恆永診所影像暫存區的權限，以此取得放射師執行檢查後之受檢客戶肺部 X 光影像。恆永診所出具之健檢報告均有醫師簽章。

4. 恆永診所於系爭合約中承諾取得至其診所進行健康檢查或癌症篩檢之客戶個人資料同意書，其中包含同意將個人資料用於進行 AI 系統分析等，以便恆永診所將客戶檢查結果等個人資料提供給智醫核心。恆永診所並無發生違反法令就個人資料進行蒐集、處理及利用之情事。

5. 於系爭合約中，智醫核心承諾確保時真 AI 系統依法取得我國醫療器材許可證，且確保其持續有效，其演算法符合醫療器材軟體查驗登記相關

指引，且軟體輸出結果涵蓋影像標記、圈選結果、罹病風險度估算、計數及分析描述等；另確保時真 AI 系統符合歐盟人工智慧法之相關規範；同時確保時真 AI 系統係以百萬筆合法授權的臨床資料進行訓練而成，並持續以合法授權資料進行更新，且具備符合醫療資訊系統業界通行之資安管理與技術控制水準，包括但不限於 ISO/IEC 27001、ISO/IEC 42001、ISO/IEC 18974、NIST AI 100-1、NIST AI 100-2 所揭示之管理與技術控制水準。

6. 恆永診所迄未導入多重驗證（MFA），測試環境與正式環境亦迄未完全隔離，且存在部分帳號共用之情形。

7. 智醫核心迄未向恆永診所提供下列文件或採取下列措施：
   7.1. 軟體物料清單（SBOM），揭露所使用之第三方開源軟體元件；
   7.2. 已知高風險弱點清冊，包含弱點類型、影響範圍與風險評估；
   7.3. 對於尚無正式修補程式之漏洞，提出具體之補償性控制措施；
   7.4. 建立完善對抗式攻擊偵測機制；
   7.5. 建立影像完整性驗證（如 hash 或簽章）。

8. 截至系爭合約簽約日，時真 AI 系統所使用之第三方開源軟體元件「EYE-CLIP」中存在已公開揭露之高風險弱點 GHSA-1a1s-30ck-te5t（下稱「系爭弱點」），尚無正式修補程式。

9. 智醫核心在訓練時真 AI 系統的過程，委託下游資料服務公司提供用以訓練的醫療資料庫以及資料標註服務，該下游資料服務公司使用了多家具有著作權的歐美醫療資料庫，進行資料標註後提供給客戶，其中包含歐美醫療資料庫 KK 的資料。KK 以獨樹一格的分析圖表、判讀報告彙整呈現方式著稱，且有獨樹一幟的「KK 智能標示系統」，此系統不僅包含特殊的色彩配置、圓周標註樣式與命名縮寫，且在所有輸出的分析圖表右下角均隱含一組由特定像素擾動組成的隱性追蹤標記，用以追蹤資料流向。此外，該系統對於其資料庫裡醫療影像的標示並未採用業界通用的醫學標準術語，而是 KK 獨創的命名縮寫法（如：K-L-TH-4-K 即代表左側第四胸椎）。

10. 智醫核心於產品上市前進行內部審查時，董事長郝安詮於 2024 年 12 月 20 日出席董事會，曾詢及時真 AI 系統訓練的臨床資料如何蒐集，列席的公司技術長口頭報告稱：「『時真 AI 系統』的資料是由專業的資料服務公司提供，該資料服務公司業務當初洽談的時候曾表示訓練資料皆取自合法來源。由於下游資料服務公司的資料來源多元，若要由本公司

就資料供應鏈再逐一為溯源審核，可能相當耗時費力」。出席董事聞言均未要求提出具體資料來源證明或授權文件，即一致通過 2025 年產品上市決議。

11. 2025 年 3 月間，甄恆永詢問時真 AI 系統可能導入之時程以及訓練資料來源，智醫核心的技術長在回覆之郵件中提及：「本公司委託下游資料服務公司提供歐美醫療資料庫以及標註服務，以提高 AI 模型正確率，且資料服務公司業務當初洽談的時候曾經表示訓練資料皆取自合法來源。由於下游資料服務公司的資料來源多元，資料供應鏈溯源審核需要花費相當時間，鑒於恆永診所希望及早導入產品，建議是否先以優化效能為首要目標，至於查證工作本公司也會進行，但不確定何時可以完成」。甄恆永回覆「以產品能於 2025 年 6 月下旬前驗收通過並得以順利使用為優先」。

12. 恆永診所於 2025 年 6 月 21 日完成時真 AI 系統之驗收，並依約出具驗收通過證明予智醫核心。恆永診所旋即開始使用時真 AI 系統評估健檢客戶之 X 光影像，並將經過時真 AI 系統處理之影像及其判讀結果提供予醫師。

13. 2025 年 9 月 11 日，一位網紅在社交媒體上爆料，聲稱恆永診所將其有小細胞肺癌初期症狀的影像誤診為正常，致使癌細胞後續轉移到淋巴腺，發展成肺癌第二期，降低其存活率。恆永診所於 2025 年 9 月 12 日展開調查，發現該網紅 7 月健檢之原始 X 光影像顯示其肺門確實有疑似結節的陰影，然時真 AI 系統呈現之 X 光影像無法看出病灶特徵，且其判讀結果為「無結節徵象」。出具報告的醫師表示，其檢閱時真 AI 系統處理之 X 光影像，認為此判讀結果無誤，故據以出具健檢報告。

14. 隨後恆永診所及智醫核心共同委託第三方調查，於 2025 年 9 月 26 日確認：有駭客侵入恆永診所伺服器後竄改 X 光影像，進一步並利用時真 AI 系統的系統漏洞進行攻擊。調查結果顯示攻擊情節如下：

    14.1. 取得恆永診所醫療影像伺服器（PACS）存取權限：駭客透過社交工程郵件使用行政人員帳號進入內網，隨後透過橫向探索，藉由系統管理員於測試伺服器留下的憑證提取管理員權限，成功進入影像暫存區伺服器（Gateway），對傳輸中的影像進行攔截。

    14.2. 自動化惡意腳本與竄改影像：駭客在影像暫存區植入腳本，利用生成式修補技術（Inpainting）對病灶區域進行微量的「特徵平滑

化」修改。影像之病灶特徵在視覺上變得極不明顯（如：邊緣模糊化）。

14.3. 利用時真 AI 系統漏洞進行攻擊：

14.3.1. 系統架構：時真 AI 系統採用 Multimodal RAG（多模態檢索增強生成)架構。其運作邏輯是由視覺模型先定位特徵，再由檢索器（Retriever）比對知識庫。智醫核心套用開源的 EYE-CLIP 預訓練模型作為檢索器，將醫療影像與診斷語義進行關聯匹配，並產生初步判讀報告。

14.3.2. 系爭弱點與對抗式攻擊：駭客針對 EYE-CLIP 模型實施「對抗式誘騙攻擊（Adversarial Evasion Attack）」。藉由在其以生成式修補技術（Inpainting）修改過影像中植入微小但具特定擾動的雜訊模式，干擾 EYE-CLIP 在特徵空間（Embedding Space）的對齊方向，迫使系統從知識庫中檢索出與真實症狀完全相反的「良性案例」作為參考依據，進而認定影像為無異常。系爭弱點已於 2025 年 4 月 18 日由官方公告，但智醫核心迄未發布系統更新修補。

15. 第三方調查確認，攻擊期間約 2 個月，期間內系統準確度遠低於衛生福利部食品藥物管理署（TFDA）核准標準。除該網紅爆料外，另有若干客戶聲稱遭誤診為正常，其肺癌症狀於此期間內惡化。恆永診所於 2025 年 10 月 3 日發布聲明並停用時真 AI 系統。恆永診所於此後半年內大量流失客戶，並已支付和解金至少新台幣二千萬元。

16. 在本次資安事件發生前，智醫核心大幅宣傳時真 AI 系統，智醫核心技術長在接受專訪時一再提到廣泛蒐羅全球各類型案例進行訓練，確保 AI 判讀完整以臻精準等。KK 台灣分支機構負責人柯仲克為恆永診所客戶，聽聞恆永診所引進時真 AI 系統後，想瞭解時真 AI 系統能發揮到何種程度，便選擇以時真 AI 系統進行肺癌判讀之健檢方案。

17. 柯仲克收到檢查報告後，發覺報告中的分析圖表在色彩配置、圓周標註樣式與命名縮寫上，與 KK 智能標示系統實質近似；經 KK 內部技術檢測後，另發現部分圖像特徵與 KK 系統所使用之隱性追蹤標記具有高度關聯。柯仲克經內部調查確認授權對象並不包含恆永診所及智醫核心，遂由 KK 委託律師向恆永診所及智醫核心寄發侵權通知函（附件 2），主張渠等疑似未獲授權使用其具有著作權之色彩配置、圓周標註樣式與

命名縮寫等。於恆永診所 2025 年 10 月 3 日發布聲明之後，KK 因發函予恆永診所及智醫核心未獲回應，續於 2025 年 10 月 16 日透過媒體公開指控恆永診所使用的時真 AI 系統，疑似未經授權擅自利用 KK 資料庫之資料。恆永診所受到外界質疑的情況日趨嚴重。

18. 甄恆永曾多次試圖聯繫智醫核心高層，擬就智醫核心所應負擔之賠償責任進行協商，然智醫核心均未回應。恆永診所乃於 2025 年 11 月 3 日向智醫核心發送律師信函，主張依照系爭合約第 5.3 條規定，立即終止雙方契約關係。嗣於 2025 年 11 月 10 日，恆永診所負責人甄恆永向臺北地方法院提起民事訴訟，提出以下主張：

    18.1. 被告違反系爭合約第 4.3 條第(7)款、第 7.3 條(1)約定及第 8.3 條約定，未依 ISO/IEC 18974: 2023 第 4.3.2 點規定，即軟體提供者於使用開源軟體時，應建立穩定且健全的弱點處理機制，包括追蹤已知弱點，並持續分析新公開之弱點，必要時應通知客戶，將早已在 EYE-CLIP 的官方 GitHub 公開之系爭弱點通知恆永診所，亦未建立適當弱點處理機制；
    18.2. 被告違反系爭合約第 4.3 條第(2)款、第(7)款及第 7.3 條(3)約定，未建立影像完整性驗證（hash 或簽章）導致未即時發現客戶 X 光片被竄改；未就時真 AI 系統建立對抗性樣本偵測導致未能即時發現駭客加入對抗式雜訊誤導 AI；
    18.3. 被告違反系爭合約第 4.6 條規定，未採行適當資安監測機制，以致無法及時發現系統準確率明顯異常，並完成模型校正等事項；
    18.4. 被告違反系爭合約第 5.2 條第(1)款規定，明知時真 AI 系統含有開源軟體 EYE-CLIP，且考量該系統用於肺癌檢測等而對健康有重大影響，仍未主動提供原告使用時真 AI 系統應知悉之資料（如：SBOM）；
    18.5. 被告違反與原告間的系爭合約第 4.3 條第(5)款及第 5.2 條第(3)款約定，未經授權即使用 KK 資料庫，係以違法取得之資料用以訓練 AI 模型，致原告遭 KK 公司指控侵權，構成產品瑕疵並使原告受有損害；
    18.6. 因被告智醫核心前開違約情節，時真 AI 系統具有重大瑕疵，構成不完全給付。

    其於起訴狀中主張：被告智醫核心未履行系爭合約約定義務，致使原告恆永診所面臨健檢客戶究責，聲譽嚴重貶損，並於其後半年內原有客戶大量流失，損害重大，乃依法請求被告智醫核心給付恆永診所新台幣 2 億元整暨自起訴狀繕本送達翌日起至清償日止，按年息 5%計算之利息，

原告並表明此為一部請求，尚保留日後擴張請求或另行訴訟之權利。

19. 本案經臺北地方法院發函請兩造提出本件爭點整理書狀，並訂定開庭期日行準備程序。原告及被告均表示並不爭執上述第 1 至 17 點所述事實，亦不爭執臺北地方法院對於本案具有管轄權。經法官協助兩造整理爭點如下：
    (1) 原告主張被告有以下違約情節，有無理由？
        i. 被告未依 ISO/IEC 18974: 2023 第 4.3.2 點規定辦理，致未能發現系爭弱點、通知原告並建立適當弱點處理機制，違反系爭合約第 4.3 條第(7)款及第 7.3 條(1)及第 8.3 條約定；
        ii. 被告未建立影像完整性驗證（hash 或簽章）導致未即時發現客戶 X 光片被竄改、未就時真 AI 系統建立對抗性樣本偵測導致未能即時發現駭客加入對抗式雜訊誤導 AI，違反系爭合約第 4.3 條第(2)款、第(7)款及第 7.3 條(3)約定；
        iii. 被告未及時發現系統準確率明顯異常，並完成模型校正，違反系爭合約第 4.6 條約定；
        iv. 被告未主動告知原告時真 AI 系統使用開源軟體 EYE-CLIP 之事實，違反系爭合約第 5.2 條第(1)款約定；
        v. 被告以違法取自 KK 資料庫之資料訓練 AI 模型，違反第 4.3 條第(5)款及第 5.2 條第(3)款約定。
    (2) 原告主張因有上開(1) i.至 v.之情節，時真 AI 系統具有重大瑕疵，構成民法第 227 條第 1 項之不完全給付，有無理由？
    (3) 原告主張其受有下列損害，依系爭合約第 5.3 條第(3)款、第 7.4 條、第 9.1 條及民法第 227 條第 1 項、第 227 條第 2 項規定，請求損害賠償，有無理由？如有，得請求之金額分別為何？
        i. 原告支付其客戶之和解金新台幣二千萬元；
        ii. 原告客戶流失之營業損失；
        iii. 原告商譽貶損之財產上及非財產上損失；
        iv. 原告因處理時真 AI 系統錯誤判讀及未經授權使用 KK 資料庫事件而支出之費用。
    (4) 原告依前開(3)所得請求之金額，是否受系爭合約第 9.2 條約定所定賠償金額上限之限制？

20. 本件承審法官諭知準備程序終結，並擬進行兩次言詞辯論期日，第一次言詞辯論期日訂於 2026 年 10 月 19 日，第一次言詞辯論期日擬就上述爭點(1)及(2)進行審理，兩造應於 2026 年 9 月 26 日以前，針對第一次言詞辯論期日審理事項提出言詞辯論意旨狀。第二次言詞辯論期日擬就上述爭點(3)及(4)進行審理，書狀提出期限及庭期另行通知。第一次言詞辯

論期日之言詞辯論意旨狀毋須就爭點(3)及(4)論述。

附件清單：

附件 1：恆永診所及智醫核心簽署之 AI 輔助診斷系統採購與授權合約（含附件甲、乙）

附件 2：KK 委託律師寄發給恆永診所及智醫核心之侵權通知函

附件 1

AI 輔助診斷系統採購與授權合約

本合約由下列雙方於 2025 年 4 月 21 日（下稱「生效日」）簽訂。

立合約書人：

甲方：恆永健康診所
機構代碼：1234567891
統一編號：22334455
地址：臺北市大安區平安路一段 20 號
代表人：甄恆永

乙方：智醫核心科技股份有限公司
統一編號：87654321
地址：臺北市信義區科研路五段 8 號 11 樓
代表人：郝安詮

基於甲方醫療服務與所內 AI 輔助判讀之需求，乙方同意提供其 AI 輔助判斷系統之安裝、授權、維運及相關服務，甲、乙雙方爰依合意約定條款如下：

第 1 條 定義

除上下文另有約定外，本合約用語定義如下：

1.1. 本系統：指乙方提供之「時真 AI 系統」及其所有必要元件，包括但不限於軟體程式、模型權重、推論引擎、管理後台、更新修補檔、文件、API、必要套件與相依項（含第三方或開源元件）。

1.2. 安裝環境：指甲方所內或甲方指定之伺服器、虛擬化環境、儲存設備與網路架構。

1.3. 受檢者：依甲方醫療或健康檢查服務而主動提供個人生物識別資料、生理資料及醫療病史，並接受甲方執行特定臨床檢驗項目之資料當事人。

1.4. 輸入資料：指甲方提供或於甲方安裝環境中產生之影像、DICOM、標註資訊、病理或檢查報告、病歷片段等必要參數。

1.5. 輸出結果：指本系統對輸入資料所生成之判讀建議、分級風險、文字報告、可視化標記、信心分數等結果。

1.6. 資安事件：指影響本系統機密性、完整性或可用性之情形，包含未授權存取、惡意程式、資料外洩、模型被植入、供應鏈攻擊、對抗式攻擊造成重大誤判、或重大漏洞利用。

1.7. 重大缺陷：指本系統出現(1)造成誤判或延誤治療風險顯著升高、(2)高風險資安漏洞、(3)核心功能無法使用或(4)違反本合約保證或法規要求之缺陷。

1.8. 重大誤判：指本系統對受檢者病情作出與實際嚴重程度明顯不符且足以影響臨床決策之錯誤判讀。

第 2 條 合約標的、價金與合作模式

2.1. 本系統採用生成式 AI 模型與影像辨識技術，協助評估胸部 X 光影像，並進行肺癌風險預測與臨床輔助判斷，及快速自動輸出判讀結果與報告。

2.2. 乙方同意將本系統採甲方地端部署(On-Premise)方式安裝於安裝環境，並授權甲方使用本系統以便判讀輸入資料並判斷健康狀態及進行癌症風險預測；甲方同意依**附件甲**之付款條件支付各類費用及款項。未經甲方同意，乙方不得請求額外報酬或費用。

2.3. 雙方瞭解本系統為輔助性工具，輸出結果不足以取代專業醫事人員之判斷。

2.4. 本合約包含下列範圍：

(1) 軟體、更新修補檔、文件、API、必要套件與相依項之授權；
(2) 安裝、部署與驗收；
(3) 維運、更新與資安修補；
(4) 技術支援與教育訓練。

第 3 條 授權範圍與限制

3.1 乙方授予甲方於合約期間內，於安裝環境內，以醫療服務用途使用本系統之非專屬、不可轉讓、不可再授權之使用權。

3.2 乙方同意甲方之人員，包括但不限於醫事人員、資訊人員及合作廠商，在必要範圍內操作本系統。

3.3 未經乙方書面同意，甲方不得將本系統提供第三人作商業服務。

3.4 甲方不得以逆向工程、拆解、還原原始碼，或以其他方式取得本系統之核心模型、權重或機密架構。甲方得為資安稽核、法遵、醫療品質管理需要，進行必要之測試、記錄與取證（含第三方滲透測試或弱點掃描），乙方不得拒絕。

第 4 條 交付、安裝、驗收與保證

4.1. 乙方須完成安裝、技術設定、測試、教育訓練並通過驗收，始得視為交付完成。

4.2. 甲方須提供符合乙方建議規格之硬體、網路、權限與資安環境（含防火牆、帳號、憑證），包括但不限於允許乙方存取甲方影像暫存區之權限。

4.3. 乙方將盡其合理商業努力維持本系統之正常運作及確保如下：

(1) 本系統之演算法符合醫療器材軟體查驗登記相關指引，且軟體輸出結果涵蓋影像標記、圈選結果、罹病風險度估算、計數及分析描述等。

(2) 本系統符合資通安全責任等級分級辦法附表十「資通系統防護基準」中針對防護需求等級為「高」資通系統之系統與資訊完整性構面中之「軟體及資訊完整性」控制措施。

(3) 本系統符合歐盟人工智慧法（EU AI Act）（如適用）之規範。

(4) 本系統係以至少一百萬筆資料進行訓練或微調。

(5) 提供本系統時，依其合理知悉與可控制範圍內，未使用違法來源之資料訓練本系統。

(6) 本系統依法取得我國醫療器材許可證並透過持續驗證及更新以維持通過主管機關驗證階段之準確率及效能。

(7) 本系統具備符合醫療資訊系統業界通行之資安管理與技術控制水準，且至少應包括 ISO/IEC 27001、ISO/IEC 42001、ISO/IEC 18974、NIST AI 100-1、NIST AI 100-2，及於合約期間維持相關資安認證之有效性。

4.4. 乙方應於 2025 年 5 月 21 日前完成本系統之安裝及於甲方安裝環境進行

測試，經甲方測試可行性並出具驗收通過證明後即為驗收完成。甲方若未於本系統安裝後一個月內提出書面不合格理由，視為驗收通過。

4.5. 若驗收未通過，乙方應於七個工作日內完成修正並重新驗收；本系統於安裝後及驗收完成前累計未通過達十次，甲方得解除合約並請求返還價金退款，且不負任何賠償責任。如甲方另受有損害，仍得向乙方請求賠償。

4.6. 於驗收通過後，乙方應實施簽約時業界一般使用 AI 系統所應採行之資安機制（包括但不限於建立效能監測機制、因應資安事件應為之偵測、監控或檢測），並於發現本系統準確率明顯異常時，完成模型校正、更新及驗證，且不向甲方收取額外費用。

第 5 條 智慧財產權與第三方權利保證

5.1. 雙方於履行本合約前既有之權利及智慧財產權等，仍各歸其原所有者。本系統及其衍生成果若含有乙方智慧財產者，乙方同意於合約期間，依據第 3.1 條無償授予甲方非專屬、不得轉讓且不得再授權之權利。

5.2. 甲方得要求乙方提出包括但不限於下列資料，乙方不得以商業機密為由拒絕提供；若乙方識別有任何資料屬甲方使用本系統需知悉之資料，乙方得主動提出，如：

(1) 軟體物料清單（SBOM）；
(2) 訓練資料來源類型說明；
(3) 合法授權或使用權利之證明；
(4) 訓練及微調資料未違反用途限制之聲明。

5.3. 如第三方就本系統主張侵權或權利爭議，乙方應自費協助處理；不論是否已有確定判決認定本系統侵害第三人權利，甲方均得終止本合約，乙方並應負擔如下責任，惟未經乙方之同意，甲方不得自行與第三人達成調解、和解或賠償：

(1) 負擔全部費用，包括但不限於賠償金、裁判費、律師費；
(2) 保障甲方及其人員免受損害，包括但不限於醫事人員、行政人員；
(3) 若甲方或其人員因此受主管機關調查、進行司法程序、遭遇媒體風險、客戶索賠等，乙方應負全部之賠償責任。

第 6 條 個人資料與醫療資料處理

6.1. 雙方同意就輸入資料及相關個人資料之處理，應遵循個人資料保護法及相關法規，且乙方為提供為本合約而代甲方蒐集、處理與利用之個人資料，雙方同意依照**附件乙**「個人資料業務委外條款」之約定辦理。

6.2. 甲方承諾將取得受檢者關於其個人資料用於進行本系統分析之個人資料同意書。

6.3. 甲方提供之輸入資料與個人資料均屬甲方控制，乙方僅於履約必要範圍內處理，且必須經過甲方認可之去識別化程序，不得嘗試對輸入資料進行再識別。

6.4. 未經甲方事前書面同意，乙方不得將輸入資料回傳至乙方或第三方環境，或用於訓練、微調或改善模型之目的。

第 7 條 資安要求

7.1. 乙方除應依第 4.3 條維持本系統具有本合約簽約時醫療資訊系統業界通行之資安管理與技術控制水準外，亦應維持本系統所使用第三方或開源套件之版本管理。

7.2. 甲方應確保本系統運作的物理與網路環境安全，防止未經授權的存取、竄改、刪除或其他影響資料完整性之行為。

7.3. 甲方得要求乙方提出包括但不限於下列資料或為以下措施，但若乙方識別有任何資料屬甲方使用本系統需知悉之資料或乙方應採取之措施，乙方得主動提供，如：

(1) 持續追蹤已知高風險弱點，並提供已知高風險弱點清冊；
(2) 對於尚無正式修補程式之漏洞，提出具體之補償性控制措施；
(3) 就影像輸入、向量化、RAG 流程與輸出結果設計必要防護措施，包括但不限於：
    (a) 對抗性樣本偵測（含不可見噪訊或浮水印型攻擊特徵）；
    (b) 影像暫存區完整性驗證（hash 或簽章）；
    (c) 模型輸出驗證與風險監控機制（含異常警示）；
(4) 於文件中揭露影像模型可能遭對抗式攻擊、資料污染或輸入異常影響之已知限制，並提供降低風險之建議設定。

7.4. 若資安事件係因本系統缺陷、設計不當、或乙方未依合約義務修補導致，相關處理成本（包括但不限於訴訟及律師費用）應由乙方負擔。

7.5. 甲方有權要求乙方於合理期間內提供本系統之相關資訊以供稽核，且如受主管機關或司法機關之要求、命令而有提出本系統相關資訊之必要者，乙方應配合辦理。

第 8 條 維護、更新與支援（SLA）

8.1. 乙方應提供合約期間內之維運服務，包含版本更新、安全修補、錯誤排除、技術支援與教育訓練。

8.2. 乙方同意於合約期間內，由乙方指派兩名人員依雙方合意之時間至甲方指定之處所進行每年四次，每次三小時之教育訓練。超過次數及時間之額外教育訓練將需另行約定。

8.3. 乙方知悉本系統存在資安事件或重大缺陷且可能影響甲方使用時，應於二十四小時內通知甲方、於七十二小時內提供修補措施，並於三十個工作日內提交調查、處理及改善報告。

8.4. 甲方如遇資安事件、重大缺陷或緊急事件等，應於知悉後二十四小時內通知乙方，並應依乙方指定之以下聯絡管道提供相關資訊，且乙方應於確認上述事件有影響甲方對於本系統之使用情形時，於七十二小時內提供修補措施，並於三十個工作日內提交調查、處理及改善報告。

第 9 條 賠償與責任限制

9.1. 如因乙方違反本合約之約定，致甲方受有損害者，乙方應負全部之賠償責任。

9.2. 除故意或重大過失外，乙方就本合約所生損害賠償責任，以本合約總價金為上限。

第 10 條 合約期間、終止與退場

10.1. 本合約自生效日起至 2029 年 4 月 21 日止有效。除非任一方於本合約訂立後四年期間屆滿前之六個月前，以書面通知不再續約，否則本約將自動延長至任一方提出終止之意思表示為止。

10.2.除本合約另有約定，若乙方發生下列情形之一，甲方得立即終止合約：
(1) 重大資安事件或重大缺陷且可歸責乙方；
(2) 重大之準確率未達或重大誤判造成受檢者或甲方權益重大風險；
(3) 乙方隱匿重大缺陷或通報不實。

10.3.若甲方發生以下情形之一，乙方得立即終止合約：
(1) 未支付第 2.1 條之相關費用及款項；
(2) 未依第 7.2 條合理維護甲方所提供本系統運作之物理與網路環境安全。

10.4.合約之終止不影響其本質上於本合約終止後仍應存續之所有權利及義務，且不影響雙方於終止前依照本合約已發生之請求權。

10.5.合約終止後，乙方應協助甲方完成退場：
(1) 卸載系統；
(2) 移交必要資料；
(3) 提供轉換系統之必要協助
(4) 刪除或返還甲方資料並出具刪除證明。

第 11 條 保密

雙方對於因本合約取得之商業機密、醫療資料、模型資訊、資安資訊等均負保密義務。如涉有資安事件，相關揭露應由甲方主導，乙方應配合但不得擅自對外發言。

第 12 條 準據法與爭議解決

12.1.本合約以中華民國法律為準據法。

12.2.因本合約所生爭議，雙方應基於誠信原則先行協商；協商不成者，以臺灣台北地方法院為第一審管轄法院。

第 13 條 其他

本合約一式貳份，雙方各執壹份為憑。

附件甲：費用與付款條款
附件乙：個人資料業務委外條款

甲方：恆永健康診所
代表人：甄恆永
日期：2025.4.21

（用印）

乙方：智醫核心科技股份有限公司
代表人：郝安詮
日期：2025.4.21

（用印）

附件甲：費用與付款條款

1. 本附件構成本合約不可分割之一部分，並規範甲方應支付予乙方之費用及相關付款條件。
2. 本合約之費用分類如下：

費用類型	計費週期	金額（新臺幣）未稅	付款條件
安裝費	首次	NTD 30,000,000	雙方完成本合約簽定、乙方提供專案管理計畫書予甲方、安裝完成並經甲方驗收完成後支付。付款期限為開立發票日後 30 天。
訂閱費	每年（生效日之次年起第一天至該年度末日）	NTD 5,000,000	本合約生效日週年起，按年開立發票。付款期限為開立發票日後 30 天。
服務費	每月	訂閱費之 2% (NTD100,000)	每月開立發票日後 30 天。
專業服務費	一次性	按需求報價	甲方提出需求後，經乙方同意，且雙方確認報價後開立發票。付款期限為開立發票日後 30 天。

3. 服務費

3.1 服務費係乙方向甲方提供之支援與維運服務之對價，包括但不限於：

(a) IT 服務台
(b) 軟體修補
(c) 技術支援
(d) 伺服器監控與管理
(e) 持續優化與改進
(f) 系統升級與更新

3.2 上述服務不影響或改變本合約服務本身之設計或功能。

3.3 服務期間與訂閱期間相同，其期間依本合約第 10.1 條之約定。

4. 專業服務費：合約範圍外服務

如甲方要求乙方提供超出本合約範圍之服務，甲方應另填妥變更需求單並依乙方報價另行計費。

附件乙：個人資料業務委外條款

本附件依據甲乙雙方所簽訂之恆永健康診所及智醫核心科技股份有限公司簽署之AI輔助診斷系統採購與授權合約（下稱「主契約」）第 6.1 條之約定，就甲方（恆永健康診所）委託乙方（智醫核心科技股份有限公司）處理個人資料之事項，訂定本附件以資遵循。乙方依主契約之約定，受甲方委託，以乙方提供之「時真 AI 系統」，處理甲方依法蒐集之醫療影像個人資料，協助進行癌症風險預測及臨床輔助判斷，並輸出判讀結果與報告（以下統稱「**AI 判讀業務**」）。就上述個人資料之蒐集、處理或利用行為，雙方同意遵守下列條款：

第 1 條、個人資料之委託範圍

1.1. 本附件之個人資料其蒐集、處理及利用行為，悉遵照個人資料保護法（下稱「**個資法**」）等相關法規之定義。

1.2. 甲方委託乙方執行 AI 判讀業務涉及有關個人資料蒐集、處理及利用範圍如下：

(1) 個人資料之特定目的（另提供法務部訂定之《個人資料保護法之特定目的及個人資料之類別》分類，下稱「**法務部分類**」）：

法務部分類	說明
一三五－資（通）訊服務 一三六－資（通）訊與資料庫管理 一三七－資通安全與管理 〇六四－保健醫療服務	(1) 以 AI 系統自動分析胸部 X 光影像，進行肺癌風險評估之運算。 (2) 生成影像判讀報告，提供臨床輔助決策之參考。 (3) 將分析結果回傳甲方之醫療影像儲存與傳輸系統（PACS）。 (4) 其他依甲方指示要求進行資料處理。

2. 個人資料之類別（另提供法務部分類）：

個資分類	法務部分類	說明
特殊個人資料（個資法第 6 條列舉之資料）	C－－－－健康紀錄	胸部 X 光影像。
一般個人資料	C〇〇－－辨識個人者	病歷號碼、就診日期、姓名、出生年月日、性別、身分證字號，其他可能直接或間接識別個人之資料。

1.3. 個人資料之處理與利用範圍：

(1) 乙方之 AI 系統以「本地端部署（On-Premise）」方式安裝於甲方指定之伺服器，資料不離開甲方之設施。

(2) 影像資料透過甲方內部網路（透過 DICOM 協定）傳輸至時真 AI 系統進行運算。

(3) 運算完成後，判讀結果回傳至甲方之 PACS。

(4) 除非經甲方書面同意，乙方不得將個人資料複製、備份或傳輸至甲方伺服器以外之任何環境。

1.4. 個人資料之處理與利用期間：自主契約生效日起，至主契約終止或屆滿之日止。

1.5. 個人資料之處理與利用地區：

(1) 中華民國境內甲方設施範圍。

(2) 除非經甲方事前書面同意，乙方不得將個人資料移轉至境外處理與利用。

第 2 條、執行 AI 判讀業務關於個人資料防護之約定

2.1. 乙方應視公司規模、營運狀況採取下列措施：

(1) 配置管理之人員及相當資源。

(2) 界定個人資料之範圍。

(3) 個人資料之風險評估及管理機制。

(4) 事故之預防、通報及應變機制。

(5) 個人資料蒐集、處理及利用之內部管理程序。

(6) 資料安全管理及人員管理。

(7) 認知宣導及教育訓練。

(8) 設備安全管理。

(9) 資料安全稽核機制。

(10) 使用紀錄、軌跡資料及證據保存。

(11) 個人資料安全維護之整體持續改善。

(12) 其他依照個資法與相關法規要求，經甲方書面通知後乙方應採取之措施。

2.2. 乙方對於其所維護或管理之個人資料，應進行相關保護措施，並應符合甲方要求及符合現今科技水準之資訊安全保護措施。乙方應依其所屬人員之工作範圍及職級，訂定不同之存取權限，並記錄所有存取紀錄。

2.3. 乙方於進行時真 AI 系統程式變更前，應先進行測試，並提出說明文件及申請（檢附相關文件，如：測試報告），並取得甲方同意。

2.4. 乙方於執行甲方所委託之業務時，應遵照個資法、甲方所制定之個人資料安全標準規範及個人資料安全相關標準作業程序為之，若有違反而造成甲方之損害，乙方應對甲方負本契約第 9.1 條之賠償責任。

2.5. 若因可歸責於乙方事由（包含但不限於：惡意程式、病毒、人員操作、複委託單位）造成個人資料外洩進而導致甲方損害，乙方應對甲方負損害賠償責任（包括但不限於訴訟費用及律師費用等）。

2.6. 乙方應依甲方指示，或於委託關係終止或解除時，應返還儲存個人資料之載體，並銷毀為履行本附件而蒐集之個人資料，且不得以任何形式留存。

第 3 條、資料安全事件通報義務

乙方於知悉個人資料遭受竊取、竄改、毀損、滅失、洩漏或其他侵害時，或乙方或其受僱人/複委託單位有違反個資法相關規定之情事時，應：

3.1. 於發現後 24 小時內，以電話、e-mail 或其他通訊工具通知甲方指定聯絡人。

3.2. 於發現後 48 小時內提交書面事件報告，載明事件起因、時間、範圍、影響人數、資料類型及已採取之應變措施。

3.3. 配合甲方及相關權責主管機關之調查與稽核。

3.4. 採取必要補救措施並持續向甲方報告事件處理進度。

3.5. 依甲方之指示方式及指示內容通知個人資料之當事人。

第 4 條、保留指揮監督事項

甲方保留指揮監督事項如下：

4.1. 乙方若有銷毀受託之個人資料時，應在甲方指派人員之監督下為之，並作成銷毀紀錄交甲方留存。

4.2. 分開委託之個人資料不得進行相互連結，若欲進行相互連結時，應事前取得甲方之書面同意後始得為之。

4.3. 乙方於委託契約解除或終止前 1 個月，應提出針對受委託期間曾接受自甲方處存取之個人資料清冊。並於契約解除或終止時，提出銷毀申請，經甲方同意後，於甲方之監督下執行。

4.4. 乙方如因故未能銷毀、交還或交給甲方指定之其他機關之證明，應列冊載明原因及保存的期間、方式，於取得甲方之同意後進行保存。

4.5. 個人資料之清冊其內容應包括交付各種紙本及電子形式之個人資料。

第 5 條、複委託

乙方若需將甲方委託之業務複委託其他廠商時，須經甲方事前書面同意。甲方若同意乙方得以複委託方式提供服務，乙方仍負有依照本附件規定履行之責任，複委託廠商因執行業務而造成甲方之損害時，乙方與複委託單位應對甲方之損害負連帶賠償之責（包括但不限於訴訟費用及律師費用等）。

第 6 條、保密協議

6.1. 乙方因履行主契約所取得或知悉甲方之個人資料，應負保密義務。

6.2. 本附件所稱之個人資料，係指甲方所擁有之個人資料，或依法律及契約應由乙方負保密義務之個人資料，不論其係以口頭、書面或電子紀錄等任何形式呈現，除經甲方事先書面同意、甲方自行公開或其他法律另有規定之情況外，乙方及所屬人員均應負保密義務，絕不洩漏、販售、交付或以其他方式予甲方以外之第三人知悉（但經甲方指定之第三人不在此限）、持有或利用，亦不得自行複製、留存而為契約目的以外之利用。

6.3. 乙方應與其所屬人員簽署保密協議。若乙方所屬人員有違反本附件有關保密義務之行為，視為乙方之違約行為。

第 7 條、委託個人資料之稽核

7.1. 乙方應依個人資料保護相關法規就受甲方委託之業務定期（每 1 年）記錄及稽核，並配合甲方之稽核業務，依甲方之指示提供相關文件，不得拒絕。

7.2. 乙方為處理委託事務而須處理或利用甲方所蒐集之個人資料時，乙方應遵守個資法之相關規定，同時對於甲方所制定相關標準作業程序，乙方亦應遵守之。甲方認有必要時，並得隨時於本附件委託事務之範圍內進行檢查，乙方不得拒絕。

7.3. 甲方若有相當之事實發現乙方及其所屬人員可能涉及違反主契約或個資法相關法令規定之行為時，乙方應盡最大努力協助甲方調查，提供所有必要之資料，並為各項必要之配合行為。

7.4. 若違反個資法係由乙方、乙方所屬人員或複委託廠商之行為所致者，乙方應協助甲方對外說明，並於所有訴訟程序中，協助甲方舉證已盡相關之個人資料防護義務。

第 8 條、違約賠償

乙方如有下列事由之一，視為違約，除應自行負擔相關之民、刑事、行政責任及損害賠償責任外（包含但不限於訴訟費用及律師費用），另應加罰懲罰性違約金新臺幣 500,000 元：

8.1. 違反本附件第 2 條關於個人資料防護之約定。

8.2. 違反本附件第 3 條關於資料安全事件通報之義務。

8.3. 違反本附件第 4 條甲方保留指揮監督事項之約定。

8.4. 違反本附件第 5 條複委託之約定。

8.5. 違反本附件第 6 條保密協議之約定。

8.6. 違反本附件第 7 條稽核之約定，經通知限期改善而未改善完成者。

第 9 條、附則

本附件為主契約之附件，具有與主契約相同之法律效力，雙方同意本附件為主契約不可分割之一部分。如本附件與主契約有任何條款之衝突或不一致者，應以本附件之規定為準，惟不影響主契約其他條款之效力。雙方如需對本附件內容進行任何修訂或變更，應以書面形式經雙方正式簽署後方為有效，口頭約定或其他非書面形式之修訂均不具法律效力。

附件 2

勝書法律事務所

受文者：　恆永健康診所即甄恆永
地址：臺北市大安區平安路一段 20 號

智醫核心科技股份有限公司
代表人：郝安詮
地址：臺北市信義區科研路五段 8 號 11 樓

發文日期：2025 年 8 月 4 日
發文字號：2025-9876543 號

主　旨：智醫核心科技股份有限公司提供恆永健康診所使用之「時真 AI 系統」，有侵害本所當事人英商 KK Co., Ltd.著作權之嫌，請於文到十日內就說明五所載事項函覆本所，詳如說明，請查照。

說　明：

一、本件係受本所當事人英商 KK Co., Ltd.（下稱「KK 公司」）之委任意旨辦理。

二、KK 公司長年深耕醫療資料之分析圖表產製及判讀報告整理與彙編技術，其所提供醫療資料庫服務範疇廣佈全球，且透過 KK 資料標示系統生成之圖表與報告設計及格式於國際大型資料庫間具有高辨識度。

三、另，KK 資料庫內資料之色彩配製、圓周標註樣式、命名縮寫法等內容均為 KK 公司具有原創性之表達，屬我國著作權法第 5 條第 1 項之圖形著作及編輯著作等，且 KK 公司乃著作人。

四、KK 公司近期發現，恆永健康診所（下稱「恆永診所」）引進智醫核心科技股份有限公司（下稱「智醫核心」）開發之「時真 AI 系統」（下稱「系爭系統」），而系爭系統所輸出之健康檢查報告中，出現疑似與 KK 公司著作實質相似之圖表及報告設計及格式。經 KK 公司內部技術檢測後，另發現部分圖像特徵與系爭系統所使用之隱性追蹤標記具有高度關聯，然恆永診所及智醫核心均未曾獲得 KK 資料庫之授權。

五、按「著作權人或製版權人對於侵害其權利者，得請求排除之，有

侵害之虞者，得請求防止之。」、「侵害著作人格權者，負損害賠償責任。雖非財產上之損害，被害人亦得請求賠償相當之金額。前項侵害，被害人並得請求表示著作人之姓名或名稱、更正內容或為其他回復名譽之適當處分。」、「因故意或過失不法侵害他人之著作財產權或製版權者，負損害賠償責任。數人共同不法侵害者，連帶負賠償責任。」著作權法第 84 條、第 85 條、第 88 條第 1 項分別定有明文。倘若經調查後，證實系爭系統有未經授權即重製、改作、編輯、公開傳輸 KK 公司著作之情事，KK 公司即得依前開條文主張權利。為釐清本件爭議並維護 KK 公司之合法權益，請恆永診所及智醫核心於函到十日內，就下列事項函覆本所：

(一) 說明系爭系統之訓練資料來源，包括但不限於直接或間接經由資料服務公司所取得之醫療影像及資料庫資料；

(二) 說明系爭系統已輸出或提供含有 KK 公司著作之相關報告內容及數量。

六、 為避免訟累，KK 公司特委託本所函達如上。倘恆永診所或智醫核心逾期未予回應或拒絕配合，KK 公司將採取一切必要之法律措施，包括但不限於提起民、刑事訴訟等，以維護其正當權益。

七、 核代函達如上，務請依限辦理。

包勝律師
勝書法律事務所
台北市文山區陽衡路 128 號 9 樓之 3
電話：886-2-0033-0888
電子郵件：service@goodd.law

包勝律師