

AI治理：國家智慧醫療戰略藍圖

建立負責任、具主權、接軌國際的醫療 AI 生態系

衛生福利部資訊處　　李建璋

NotebookLM

從「固定工具」到「駐院醫師」：生成式 AI 的治理挑戰

典範轉移：為何我們需要新的治理框架？

傳統判別式 AI (Discriminative)

- **定位**：訓練完成即固定的輔助工具
- **核心應用**：風險分層 (Risk stratification)、電腦視覺分類
- **生命週期**：靜態 (Static lifecycle)
- **治理焦點**：單次驗證與準確度測試

生成式 AI (Generative)

- **定位**：需持續學習與監督的「住院醫師」
- **核心風險**：幻覺 (Hallucination)、提示詞注入攻擊 (Prompt Injection)
- **生命週期**：動態 (Requires continuous lifecycle management)
- **治理焦點**：隱私外洩風險 (Prompt中夾帶個資)、持續再教育與再稽核機制

NotebookLM

國家智慧醫療生態系：三大中心架構

第一類中心：負責任 AI 中心 (Foundation)

核心任務: 建立透明度、資安防護與生命週期管理，確保 AI 輔助決策的安全性。



第二類中心：外部驗證與國家聯邦學習 (Engine)

核心任務: 發展多模態國家主權 AI，落實「資料不出院」的跨院聯合訓練。

第三類中心：臨床價值驗證與隨機試驗 (Output)

核心任務: 執行次世代 AI 臨床試驗，橋接 TFDA 認證與健保給付、國際市場准入。

NotebookLM

第一類中心：生成式 AI 的持續性生命週期管理



1. 透明化登錄 (Transparent Registration)

所有深耕計畫研發之 AI 應用，必須納入「國家臨床 AI 註冊網站」登錄，建立全國應用透明度。

2. 主權雲與資安防護 (Security & Privacy)

採用主權雲架構 (Sovereign Cloud)，防範 Prompt Injection 惡意攻擊與 Prompt 個資外洩，確保模型不濫用病歷資料。

3. 持續再驗證 (Continuous Validation)

Shadowing (影子測試)：系統後端同步執行，與人類醫師實際判斷結果進行無縫比對。

總指導官稽核：由 AI 總指導官 (AI Chief) 進行定期抽查與品質審查。

NotebookLM

負責任 AI 中心：認證與輔導軌跡

Step 1: 申請與資料準備
(Application)

[10月] 開放申請。醫院啟動院內盤點作業。

Step 2: 管理中心輔導
(Mentorship & Readiness)

確認院內設立 AI 管理委員會。
制定 AI 使用規範與透明性指標。
完成可解釋性分析與生命週期管理機制建置。

Step 3: 實地訪查與授證
(On-site Visit)

由衛福部資訊處、工研院 (ITRI) 及第一期優秀代表組成訪查團隊。
確認實際執行成效後，由衛生福利部正式授證。



NotebookLM

第二類中心：國家聯邦學習平台與跨院資料聯盟

「資料不出院，模型跨院練」
(Data stays, Models move)

跨院聯盟機制

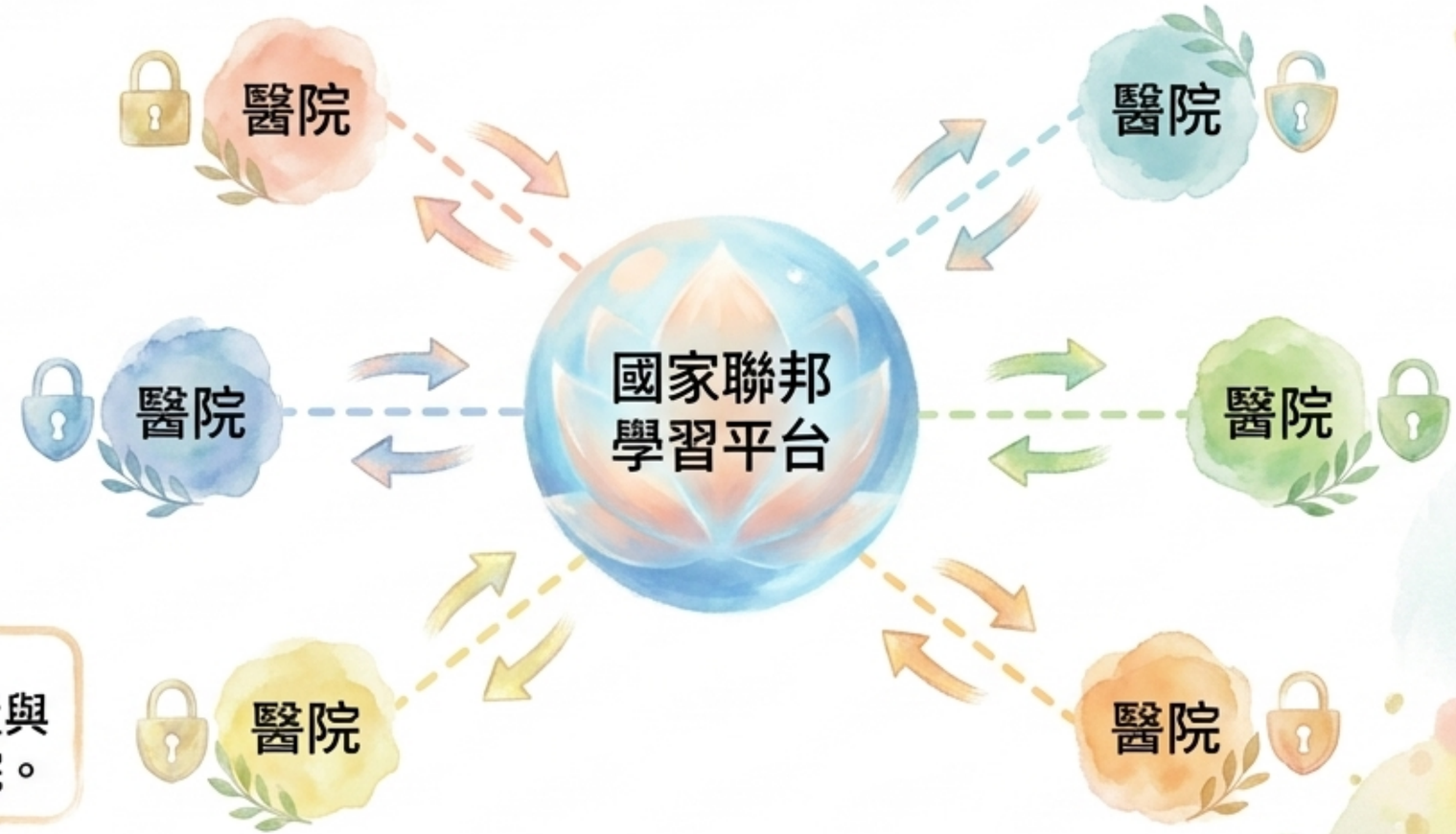
建立跨院聯盟委員會，建置標準化 FHIR 研究資料庫。

國家聯邦學習平台

作為模型訓練的協作核心，確保資料治理原則下的安全訓練。

深耕計畫資源挹注

支援相關硬體設備採購、人力配置與資料庫建置，賦能參與聯盟之醫院。



NotebookLM

打造多模態國家主權 AI (Sovereign AI)



優先落地應用

參與聯盟並配合訓練的主體醫院，將成為首批受益者，優先將國家級主權 AI 模型導入院內，發展下游智慧醫療應用。

NotebookLM

第三類中心：從 TFDA 認證到健保給付的推進引擎



NotebookLM

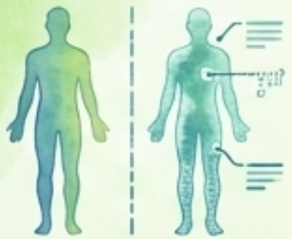
科技驅動：次世代 AI 臨床試驗方法學



適應性試驗設計
(Adaptive Design)

應用場景：罕見疾病或困難收案之 AI 應用。

優勢：動態調整試驗參數，大幅提升臨床試驗效率。



模擬對照組
(Simulated Control)

應用場景：需大量對照受試者的傳統試驗。

優勢：透過生成式數位資料建立基準線，有效降低真實對照受試者的人數需求。



嵌入式實用型試驗
(Embedded Pragmatic Trial)

應用場景：真實世界醫療環境 (Real-World Setting)。

優勢：將隨機化機制直接嵌入電子病歷系統，以最低程度影響臨床工作流程。

搭配全數位化工具（電子病歷摘要、臨床登錄系統、電子化知情同意書 e-Consent），
全面告別傳統純人工研究流程。

NotebookLM

台灣智慧醫療國家隊：接軌國際與雙向互信



Outbound Integration

- 國家隊成軍：整合一、二、三類中心優秀代表與負責人，展現實力。
- 國際展出：領軍參與 HIMSS, DMEA 等全球頂級醫療科技展。
- 跨國聯邦學習：透過國家聯邦學習中心，逐步串接歐洲、亞洲與美洲醫療機構。

Inbound Trust

國際大廠信任沙盒：當國際頂尖 AI 技術欲導入台灣市場，國家認證之二、三類中心將成為最可靠的技術與臨床驗證場域，建立雙向互信機制。

NotebookLM