健康資料與生成式AI研究倫理（三）

～臺大醫院倫理中心研究倫理研習會紀要

講者 / 臺大醫院麻醉部 葉育彰
整理 / 倫理中心 王劭慈

伍、生成式 AI 應用與挑戰：臺大醫院麻醉部葉育彰主任

本場講座中，臺大醫院的葉育彰主任分享了生成式 AI（Generative AI）在醫療與研究領域的快速發展、潛在風險、法規挑戰與未來展望。他以實務經驗與幽默的語氣，帶領聽眾理解這項技術如何在短時間內改變研究與臨床生態，同時也提醒必須在安全與倫理的基礎上前進。

一、技術的爆發成長

葉主任表示生成式 AI 的進展速度前所未有。過去做醫學研究，一個月不看新論文不至於落伍，但生成式 AI 每週都有突破，若不跟上進度，很快就會被淘汰。

他舉例，許多研究團隊花一個月開發的模型，可能在新一代模型問世後瞬間被超越。GPT 系列從 3.5 版到 GPT-4、GPT-4o，再到 GPT-o1，o3 和 o4，功能持續升級，GPT-5 亦已於 2025 年 8 月推出。

醫學界也在積極跟進，像《NEJM》早在 2023 年就開始討論生成式 AI 的優勢、限制與風險。GPT 在各國醫師國考的表現也突飛猛進，從 GPT-3.5 只能勉強及格，到 GPT-4 進入前 5%，顯示 AI 在專業知識上的學習能力驚人。

二、潛在風險與法規挑戰

生成式 AI 帶來便利，也伴隨不少風險：

1. 錯誤資訊： AI 有時會「一本正經地胡說八道」，生成看似合理但實際錯誤的內容，甚至早期連提供的參考連結都可能是假的，必須謹慎查核。
2. 隱私與資安疑慮： OpenAI 曾因大量爬取網路資料而備受批評，擔心使用者個資在不知情下被收集。

3. 法規落後：現行法律並未跟上生成式 AI 的發展，醫療領域對於病人資料的使用、安全與跨境傳輸，仍缺乏明確規範。
4. 社會與經濟影響：程式設計、文書撰寫等重複性工作正被 AI 取代，醫療研究助理與資訊人員的角色與技能需求也在改變。

醫院與資訊部門目前正嘗試建立封閉且安全的運算環境，例如與微軟合作，在台灣境內建置機房，確保醫療資料不會離開國內，並符合個資法規要求。

三、開源與封閉模型的抉擇

生成式 AI 發展出兩種路線：

1. **開源模型（Open Source）：**程式碼與模型公開，成本低、易於修改，但也可能被惡意利用。
2. **封閉模型（Closed Source）：** 由大型公司維護，性能強大、安全性高，但需要高昂的運算成本與授權費用。

在醫療場域，院內多採用「封閉的運算環境」結合「開源模型」的做法：所有含有病人個資的資料必須保留在院內，不得外流。近來微軟已在台灣設立本地機房，讓資料能在境內完成運算，降低資安疑慮。若指定資料僅在台灣機房處理，雖可能增加部分成本，卻可讓倫理委員會與研究單位更安心，確保研究在合法合規的基礎上進行。

四、臨床應用與創新契機

生成式 AI 在醫療的應用正快速擴展，包含：

- 臨床決策支持：結合機器學習（ML）與大型語言模型（LLM），可預測加護病房病人死亡風險，並提供風險因子的解釋與建議。
- 醫療文書處理：自動生成病人家屬說明書，語言精簡、同理心強，減少醫師的文書負擔。
- 研究與教育：協助文獻整理、統計分析，甚至可用於醫學生與住院醫師的教學輔助。

國際期刊已提出九項生成式 AI 醫療倫理原則，涵蓋隱私、透明度、責任歸屬等面向。台灣未來也需建立對應的審查與管理機制，讓 AI 在保障個資與臨床安全的前提下發揮最大效益。

五、未來發展與代理人時代

生成式 AI 正逐步邁向「代理人」(Agent) 時代。未來的 AI 不只回應問題，還能自動調用各種工具與資料庫，完成複雜任務，像鋼鐵人中的「賈維斯」一樣，成為研究與臨床的智慧助理。

葉主任指出院方與資訊室正合作建立標準化的審查與部署流程，確保未來的 AI 研究在台灣本地機房、封閉式環境與倫理委員會監督下運行。這一兩年可能是關鍵轉折點，研究計畫的審查、醫療決策的支援，都必須要求 AI 的運算流程透明、可追溯，確保技術在安全與倫理的框架下運作。

六、結語

生成式 AI 讓醫療與研究領域面臨前所未有的轉型。從技術突破、臨床應用到法律與倫理挑戰，未來的關鍵在於如何在創新與規範間取得平衡。正如葉主任所言：「只有在安全與規範的基礎上，生成式 AI 才能成為醫療發展的正向力量。」

(感謝講師授權記錄演講內容與季刊刊載，著作權與智慧財產權歸屬講師本人)