

行政院及所屬機關(構)使用生成式 AI 參考指引簡介

文 / 臺大醫院倫理中心 戴君芳

壹、前言

你使用 ChatGPT 了嗎？這是近期最常聽到的問話之一了。這一年多來，AI 呈現爆發式成長，也影響了我們周遭的事物，2022 年底 ChatGPT (GPT-3.5 版本) 公開後，短短二個月時間就有全球 1 億以上的用戶數使用。在一年前，您會想到一年後使用 AI 可以幫我們寫邀請信，可以幫我們蒐集資料或修改文章嗎？現在的 AI 都做得到了，且會有越來越多功能，省卻了很多耗費腦筋的事，工作效率也變高了。但在大家開始使用這麼多優點的工具時，是否會有可能的缺點及風險呢？如果大家把自己機構重要的資料、病歷資料，甚至國家的機密文件都丟入 ChatGPT 中，幫助自己的工作程序，這對機構甚至國家都可能造成洩漏機密資料的重大風險，因此行政院很快於 2023 年 8 月 31 日通過國科會制定的「行政院及所屬機關 (構) 使用生成式 AI 參考指引」[1][2]，提供了政府所屬各機關使用時遵循的原則。國科會也說明後續將觀察全球 AI 發展趨勢與因應作為，持續滾動修正此指引，使規範保留彈性，促進使用生成式 AI 之風險管理與創新發展之間取得平衡。身為政府機關所屬機構一員，我們來了解指引之重要內容包含哪些。

貳、行政院及所屬機關 (構) 使用生成式 AI 參考指引

本參考指引共計十點如下：

- 一、為使行政院及所屬機關 (構) (以下簡稱各機關) 使用生成式 AI 提升行政效率，並避免其可能帶來之國家安全、資訊安全、人權、隱私、倫理及法律等風險，特就各機關使用生成式 AI 應注意之事項，訂定本參考指引。
- 二、生成式 AI 產出之資訊，須由業務承辦人就其風險進行客觀且專業之最終判斷，不得取代業務承辦人之自主思維、創造力及人際互動。

- 三、製作機密文書應由業務承辦人親自撰寫，禁止使用生成式 AI。前項所稱機密文書，指行政院「文書處理手冊」所定之國家機密文書及一般公務機密文書。
- 四、業務承辦人不得向生成式 AI 提供涉及公務應保密、個人及未經機關（構）同意公開之資訊，亦不得向生成式 AI 詢問可能涉及機密業務或個人資料之問題。但封閉式地端部署之生成式 AI 模型，於確認系統環境安全性後，得依文書或資訊機密等級分級使用。
- 五、各機關不可完全信任生成式 AI 產出之資訊，亦不得以未經確認之產出內容直接作成行政行為或作為公務決策之唯一依據。
- 六、各機關使用生成式 AI 作為執行業務或提供服務輔助工具時，應適當揭露。
- 七、使用生成式 AI 應遵守資通安全、個人資料保護、著作權及相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性。各機關得依使用生成式 AI 之設備及業務性質，訂定使用生成式 AI 之規範或內控管理措施。
- 八、各機關應就所辦採購事項，要求得標之法人、團體或個人注意本參考指引，並遵守各機關依前點所訂定之規範或內控管理措施。
- 九、公營事業機構、公立學校、行政法人及政府捐助之財團法人使用生成式 AI，得準用本參考指引。
- 十、行政院及所屬機關（構）以外之機關得參照本參考指引，訂定使用生成式 AI 之規範。



行政院網頁

參、對本指引重點之介紹與分析

這份指引提供了一個明確的框架，幫助我們了解在政府機構內部使用生成式 AI 的相關規範和限制。以下簡介其重點。

一、行政院及所屬機關（構）使用生成式 AI 參考指引適用哪些機關？

依指引名稱，本指引之適用對象為行政院及所屬機關（構），但指引中也明列「公營事業機構、公立學校、行政法人及政府捐助之財團法人使用生成式 AI，得準用本參考指引」，因此也包含教育部所屬的本院。指引內並說明「各機關得視使用生成式 AI 之業務需求，參酌本參考指引另訂使用規範或內控管理措施」。

二、什麼是生成式 AI？

指引內參考歐盟之定義，說明「生成式 AI 模型是一種電腦程式，旨在創建類似於人類製作（human-made）的新內容。」市面上常見的生成式 AI 工具例如最為人知的 ChatGPT，其他如 Bard、Midjourney、Bing...等都各有其特色。

三、為什麼要制定使用生成式 AI 參考指引？

指引第一項說明制定使用生成式 AI 指引的目的，「為使行政院及所屬機關（構）（以下簡稱各機關）使用生成式 AI 提升行政效率，並避免其可能帶來之國家安全、資訊安全、人權、隱私、倫理及法律等風險」。因指引內明白提到了生成式 AI 的風險，「因其大量蒐集、學習與產出之資料，可能涉及智慧財產權、人權或業務機密之侵害，且其生成結果，因受限於所學習資料之品質與數量，而有可能真偽難辨或創造不存在的資訊」，因此有必要制訂參考指引供大家遵循。

四、業務承辦人使用生成式 AI 的原則及禁止事項

生成式 AI 工具有很多優點，像是提升行政效率等，也因此必須避免大家過於仰賴使用生成式 AI，指引第二項重點即說明「生成式 AI 產出之資訊，須由業務承辦人就其風險進行客觀且專業之最終判斷」。因此不論業務是否使用生成式 AI，所產出的結果都需由業務承辦人負完全的責任。也由於其產出資訊的正確性難以判斷，指引第五項亦明定「各機關不可完全信任生成式 AI 產出之資訊，亦不得以未經確認之產出內容直接作成行政行為或作為公務決策之唯一依據」。

指引第三項強調「製作機密文書應由業務承辦人親自撰寫，禁止使用生成式 AI」。這項指引明確說明禁止執行的範圍，在醫院端，病歷屬敏感性資料，2023 年 10 月 9 日衛福部醫事司劉玉菁副司長亦指出醫師法第十二條規定，醫師應親自製作

病歷，親筆撰寫或電腦打字都行，但不能用軟體產生病歷，畢竟涉及病患隱私，務必避免 AI 把病歷上傳到健保資料庫以外的地方 [3]。因此在此提醒使用時務必注意禁止使用生成式 AI 製作機密文書或書寫病歷。

五、使用生成式 AI 之注意事項

指引第四項進一步說明「業務承辦人不得向生成式 AI 提供涉及公務應保密、個人及未經機關（構）同意公開之資訊，亦不得向生成式 AI 詢問可能涉及機密業務或個人資料之問題」。由於上傳的資料可能會被納入訓練而有機密外洩的風險，媒體亦報導有部分國際大廠在 ChatGPT 的回應發現公司內部資訊，因而禁止或限制員工使用 ChatGPT，因此須特別注意此項要求。惟並非完全不得使用於涉及機密業務或個人資料上，指引亦說明「封閉式地端部署之生成式 AI 模型，於確認系統環境安全性後，得依文書或資訊機密等級分級使用」。

什麼是封閉式地端呢？在國科會網頁常見問答（FAQ）[4] 特別說明「封閉式地端」係指機關內不與外部網路連線或資料交換之地端環境，若機關採租用運算資源方式建置生成式 AI 應用，其租用之環境必須符合以下兩項條件，即視為「封閉式地端」：

1. 運算環境座落於臺灣且虛擬主機為租用者及其限定使用者專屬使用。
2. 租用者及其限定使用者採 VPN 或專線方式連入、使用該運算資源。

此項規範可供各機構在建構生成式 AI 時列為條件，以保護機構機密性之資料。另外，指引第六項也明定「各機關使用生成式 AI 作為執行業務或提供服務輔助工具時，應適當揭露」，使接受資訊者可了解其資料來源。

六、使用生成式 AI 應遵循之規定及可能之侵害

指引第七條提醒「使用生成式 AI 應遵守資通安全、個人資料保護、著作權與相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性。」

由於資料輸入生成式 AI 時，若含可辨識個人資料或本院之智慧財產權與著作權資料等，即可能有外洩的疑慮，或是大家在使用生成之資料時，並無法確認其資料來源，雖說 ChatGPT 對其產出文字不會要求智慧財產權，但資料來源之所有權人有可能主張具有智慧財產權，而致侵害其權利，因此提醒在使用生成式 AI 時，須檢視及注意輸入或輸出之資料有無上述可能之侵害，避免上述疑慮。

肆、結語（進行人體研究時的提醒事項）

近期隨著生成式 AI 工具的熱門，亦興起使用生成式 AI 進行人體研究的熱潮，期待能協助研究之發展，但由於人體研究常涉及病歷資料之使用或受試者之個人資料，依據上述指引，提醒研究者務必注意是否符合指引內容。若研究計畫使用生成式 AI，在送審研究倫理審查前，建議先評估計畫中擬輸入生成式 AI 的資料是否涉及公務應保密、個人及未經機關（構）同意公開之資訊？若屬病人資料，是否已刪除可辨識個人資料（可參考刪除美國 HIPAA 定義的 18 種 identifiers），且研究者藉其知識能力亦無法識別特定個人的身分？若含機密資料，是否屬封閉式地端部署之生成式 AI 模型？封閉式地端部署之安全性是否有經過檢驗？使用之資料是否可能造成智慧財產權或人格權之侵害？...等，以供評估是否符合研究倫理及相關資訊安全規範。只要事先做好相關保護措施，相信科學發展及受試者權益都能雙贏。

參考文獻

1. 行政院及所屬機關（構）使用生成式 AI 參考指引 行政院全球資訊網 <https://www.ey.gov.tw/Page/448DE008087A1971/40c1a925-121d-4b6b-8f40-7e9e1a5401f2>
2. 行政院及所屬機關（構）使用生成式 AI 參考指引 國家科學及技術委員會 <https://www.nstc.gov.tw/folksonomy/list/c79bf57b-dc94-4aff-8d14-3262b5559cfc?l=ch>
3. 吳亮儀等：96 件取得許可、百餘件申請中 AI 醫材進入軍備競賽 / 送審多屬中風險性醫材 衛福部強調禁用生成式病歷，自由時報，2023 年 10 月 9 日，<https://news.ltn.com.tw/news/life/paper/1608972>
4. 行政院及所屬機關（構）使用生成式 AI 參考指引 常見問答(FAQ) 國家科學及技術委員會網頁 <https://www.nstc.gov.tw/folksonomy/detail/d21566a0-3465-4b63-84b7-5d7cb2e1e5ff?l=ch>