

健康台灣深耕計畫

規劃及執行資安治理、資料治理及 AI 治理之注意事項說明

一、資安治理

資安治理重點應強化醫院整體資安韌性與主動防禦能力。

(一) 建立完整且可實際執行的備援計畫

面對日益增加的資安威脅，醫院不能只著重於事前防護，更需要確保在遭遇重大資安事件時，能夠快速恢復醫療服務。因此，異地備份、雲端備份，以及具備切換能力的雙活系統，建議納入深耕計畫的重要工作。

(二) 第針對醫院核心系統進行 Claude Mythos 安全檢測

尤其是重度級急救責任醫院以上等級的醫療機構，應與資安專業廠商合作，取得相關雲端安全 Claude Mythos 掃描服務，針對最重要的核心醫療資訊系統進行弱點掃描。因應未來人工智慧模型大量開源與快速發展後，可能帶來的新型態資安風險。當更多攻擊者利用 AI 工具進行漏洞探索時，醫院核心系統可能面臨更大規模的攻擊。因此，透過定期弱點掃描，及早發現並修補漏洞，是深耕計畫中非常重要的工作項目。

(三) 加強使用者權限管理與主動行為偵測

許多醫療資訊安全事件發生的原因之一，是因為系統管理權限過大，導致帳號被濫用、權限遭盜用。因此，醫院可利用深耕計畫資源，強化帳號權限控管、最小權限管理，以及使用者行為分析與異常偵測機制。相關作法可以參考衛生福利部資訊處所發布的資訊安全管理相關指引，建立更完善的權限治理制度。

(四) 勒索軟體演練與教育訓練

其中最重要的是勒索軟體防禦能力。勒索軟體目前仍是台灣醫療體系最大的資安威脅之一，因此所有醫院資訊人員都應具備第一時間的事件應變能力，包括攻擊發生時的判斷、隔離、損害控制、系統復原，以及事件通報流程。因此，在深耕計畫的資安範疇中，建議納入勒索軟體演練與教育訓練，提升醫院整體應變能力。

(五) 主權雲治理模式

因應生成式 AI 與雲端應用快速發展，醫院若將病人資料應用於雲端 AI 服務，涉及個人資料與醫療資料安全問題，因此應建立主權雲服務模式。醫院與雲端服務業者合作時，應簽訂符合資料主權與安全要求的相關合約，合約內容可參考衛生福利部所公布的相關草案與規範。

(六) 投入先進資安科技

深耕計畫資源亦鼓勵投入先進資安科技，包括利用人工智慧進行主動式資安監控、導入 MDR（Managed Detection and Response）或 XDR（Extended Detection and Response）等偵測與回應服務，以及強化資料保護措施。其他相關高科技資安建置項目包括：備份資料加密、智慧化網段管理、不可被刪除或竄改的不可抹除備份機制（Immutable Backup）、異地雙活系統建置，以及零信任架構（Zero Trust Architecture）的導入。

透過這些措施，醫院才能從傳統被動防禦模式，逐步轉型為具備主動偵測、快速應變與持續復原能力的新世代智慧醫療資安體系。

二、資料治理

資料治理的部分，鼓勵利用深耕計畫資源導入衛生福利部所推動的 FHIR Box，進行醫療資料標準化與互通性建置。FHIR Box 是本部資訊處開發新一代跨平台的醫療資訊互通作業系統。它除了可以協助醫院將既有資料轉換成標準化

的台灣核心資料群（TWCDI）格式之外，也能進一步連接醫療資料生態系。目前衛生福利部已公告相關應用方向，未來應該以台灣健康資料空間（Taiwan Health Data Space），台灣健康規則空間（Taiwan Health Rule Space）以及台灣健康應用空間（Taiwan Health App Space）等生態系為主要發展方向。

目前衛生福利部資訊處所提供的 FHIR Box 示範環境，主要仍屬於技術驗證的示範(Proof of Technology)。因此，三級醫院可以利用深耕計畫資源，規模化全院導入 FHIR Box，進行自身院內資料轉換與標準化，才能真正促進全國醫療資料的大規模轉換與互通。完成資料標準化、跨院互通，以及未來生態系應用。

FHIR Box 不只是單純的資料轉換工具，而是協助醫院進行全院級資訊架構升級的重要基礎建設。衛生福利部資訊處將公告符合資格的資訊服務廠商，以及相關硬體設備供應商，醫院可以選用衛福部認證廠商推動建置。

(一)台灣健康資料空間（Taiwan Health Data Space, THDS）

THDS 是一個提供全國交換 TWCDI 台灣核心資料群的資料空間，所提相關範疇三計畫中，如果使用到 TWCDI 沒有規範的資料，可以依 HL7 國際相關 IG 新增 Taiwan Core Plus 台灣擴增核心資料群 FHIR 標準（FHIR Implementation Guide），相關標準應送至台灣醫療資訊標準大平台進行審查與公告。如果有全國一制性質，希望納入成為國家標準（TW Core IG），則需要申請由跨領域專家委員會進行審查，確認其符合國家醫療資料標準後，再正式公告。透過深耕計畫，各界編制更多的 FHIR 標準，深化國家醫療資料治理，產出和國際接軌的台灣 FHIR IG，視為是深耕計畫資訊領域重要目標。

(二)台灣健康規則空間 (Taiwan Health Rule Space, THRS)

台灣健康規則空間是指透過 FHIR Box 標準化醫院資料後，就可以導入標準邏輯規則，完成醫院相關行政自動化，表達邏輯規則的程式語言是 CQL (Clinical Quality Language)，這是一項由美國 AHRQ 發展出來，與 FHIR 資料原生的程式語言，可以協助醫院建立各種應用將公共衛生監測、健保申報、自動病歷審查、實證醫學分析，以及醫療品質管理等等流程自動化，結合 CDS Hooks (clinical decision support hooks) 的技術，則可以做成 Clinical Decision Support 系統內嵌於醫院 HIS。因此，深耕計畫可以利用資源，在 CQL 與 FHIR 的架構下發展臨床決策支援系統 (Clinical Decision Support System)，透過標準化規則與 FHIR Box 內建的 ELM 引擎執行 CQL，讓醫療品質管理、健保規範與公共衛生工作能夠自動化。醫院對於 CQL 技術不熟，可以透過衛生福利部認證具 CQL 能力廠商協助建置。此外政府也會將各計畫完成的開源 CDS 放置於 TWRS 內建於 FHIR Box，相關 CQL 規則也應送交次世代電子病歷執行計畫辦公室進行審查與上架，讓深耕計畫中各醫院產生的研究成果與應用成果，逐漸累積成為國家的醫療數位資產。

(三)台灣健康應用空間 (Taiwan Health App Space, THAS)

所有深耕計畫所衍生的應用程式，都必須符合資料標準要求。資料部分必須符合台灣核心資料群 (TWCDI) 的定義，才能真正達到全國通用。同時，所有深耕計畫產出的應用程式，都應該依照國家市集規範上架。應用程式必須符合 SMART on FHIR 標準，才能進入國家級醫療應用生態系。因此，所有醫院，包括區域醫院、地區醫院與醫學中心，皆可利用深耕計畫資源，透過台灣自主技術 FHIR Box 完成資料標準化，建立國家電子病歷互通基礎。

此外，所有應用程式應該以 SMART on FHIR 形式封裝，鼓勵形成訂閱型服務模式，促進醫療應用生態系發展。應用程式所使用的資料，必須符合台灣核心資料群規範；如果需要延伸資料模型，則可提出 Implementation Guide (IG) 延伸，而 IG 延伸責任由開發廠商負責，審查則由國家電子病歷標準相關單位負責。透過這樣的架構，深耕計畫所產出的應用服務，才能真正從單一醫院成果，轉化成全國共享、可持續發展的智慧醫療生態系。

相關 SMART 標準規範、技術文件與操作手冊，也可以透過台灣健康 App 或相關平台進一步學習與推廣。避免深耕計畫再次投入重複性的應用程式開發，而應在國家市集上訂閱已開發程式，在醫院落地，促進應用程式訂閱經濟的發展。因為開發一個完整應用程式所需投入的資金與時間，遠高於透過訂閱模式使用成熟應用服務的成本。因此，深耕計畫的資源建議應著重於建立共同底層標準，讓各醫院與開發者可以在共同平台上發展應用，而不是每一家醫院各自重複建置。

三、AI 治理

如果醫院在深耕計畫中推動 AI 相關應用，尤其是智慧醫療軟體 (Software as Medical Device, SaMD) 的發展，未來若希望申請 TFDA (衛生福利部食品藥物管理署) 醫療器材認證，建議應充分利用國家 AI 外部驗證中心的資源，透過大規模、具有人群代表性的真實世界資料進行驗證。

AI 模型不能只在單一醫院或少量資料中驗證，而應該透過跨醫院、跨族群的大規模資料，確認模型在真實臨床環境中的效能與安全性。此外，也可以透過國家聯邦學習平台 (Federated Learning) 架構，利用全國性的醫療資料進

行模型驗證與優化，在不移動病人資料的前提下，提升 AI 模型的泛化能力。醫院可以利用深耕計畫建置軟硬體成為國家聯邦學習網路節點，讓院資料納入國家主權 AI 訓練達成數位平權。

深耕計畫的資源亦可以協助醫院建置 GPU 高效能運算設備，讓醫院能加入全國性的聯邦學習網絡，未來進一步參與國家主權 AI 訓練計畫，建立台灣自主的醫療 AI 發展能力。

另外，對於已經在醫院落地實施的 AI 系統，所有深耕計畫所導入的 AI 應用，都應該納入國家 AI 註冊管理平台進行登錄與註冊，並且依循負責任 AI（Responsible AI）的精神，建立完整的管理、監督與運作機制。未來政府也將建立 AI 治理與註冊管理工具，協助醫院進行 AI 使用管理，包括模型來源、用途、適用範圍、效能監測、風險管理等，確保 AI 在醫療場域中安全且透明地運作。

另一方面，若深耕計畫所發展的 AI 模型已經取得 TFDA 認證，或者尚未取得 TFDA 認證但具有商品化潛力，深耕計畫建議應協助提升台灣智慧醫療在國際上的影響力。

其中一個重要策略，就是鼓勵利用深耕計畫資源進行隨機臨床試驗（Randomized Controlled Trial, RCT），取得高品質臨床證據。透過科學嚴謹的驗證，不僅可以支持 AI 產品取得法規認證，也能為未來健保給付政策、臨床實證指南（Clinical Practice Guideline）的制定提供關鍵依據。

未來若要推動相關 AI 隨機臨床試驗，可以與本部資訊處所支持的五大 AI 中心合作申請，將深耕計畫資源投入多中心臨床驗證。此外，如果民間企業希

望推動 AI 醫療產品的臨床驗證，也可以結合經濟部中小企業相關輔導資源，並與第三類醫療器材臨床試驗中心合作，建立產官學共同驗證模式。透過這樣的方式，可以讓更多成熟的智慧醫療產品接受高科學品質驗證，產生更具國際競爭力的成果。

因此，深耕計畫在 AI 治理部分的重要方向如下：

- (一) 建立國家型 AI 落地註冊網站，以及負責任 AI 管理工具，讓所有進入醫療場域的 AI 應用都有完整管理機制。未來也會公布相關認證制度，醫院可以利用深耕計畫資源申請成為負責任 AI 中心，建立 AI 治理能力。
- (二) 深耕計畫產出的 AI 模型，如果希望未來透過商業化方式推廣到全國使用，應鼓勵取得 TFDA 認證。而在取得認證過程中，利用深耕計畫資源，透過國內 AI 外部驗證中心，以具有人群代表性的資料進行驗證，避免因資料偏差造成數位不平權。

國家 AI 外部驗證中心除了可以整合跨領域、跨醫院的 FHIR 標準化資料庫，協助 AI 模型驗證之外，也可以透過國家聯邦學習平台協助模型訓練、驗證與優化，加速 AI 產品取得 TFDA 認證。

同時，也鼓勵醫院利用深耕計畫資源加入既有的國家 AI 驗證網絡，包括聯邦學習網絡與 FHIR 資料網絡，讓台灣 AI 外部驗證中心的規模持續擴大。

最後，深耕計畫亦可協助醫院產出具有國際影響力的高品質研究成果。透過廣泛推動多中心隨機臨床試驗，不僅取得高品質國際論文，也能累積未來健

保給付與醫療科技評估（Health Technology Assessment, HTA）所需要的本土臨床證據。同時，多中心隨機臨床試驗也可以結合經濟部相關資源，建立未來實證醫學指南所需要的本土化、高品質科學資料，讓台灣智慧醫療發展不只是技術導入，而能建立完整的臨床證據與國際影響力。