人工智慧醫療器材優良機器學習實務：開發與管理原則

115 年 6 月 4 日

一、 前言

隨著人工智慧與機器學習技術在醫療器材領域的蓬勃發展，確保其安全、有效且具備優良性能已成為全球產品開發與管理的核心。本署參考國際醫療器材主管機關論壇(IMDRF)所發布之「Good machine learning practice for medical device development: Guiding principles」[1]及相關標準與指引文件[2-15]，擬定「人工智慧醫療器材優良機器學習實務（Good Machine Learning Practice, GMLP）」十項原則，範疇涵蓋產品設計、軟體工程品質、資料集代表性及上市後性能監控等全生命週期管理。透過落實本原則，有助於業者發展切合臨床實務的產品，有效管理演算法偏差與資料漂移等潛在風險，以及機器學習技術迭代特性所產生之風險。業者得視本身產品宣稱效能、適用範圍、對象及使用情境等評估本原則內容之適用性，以採取最符合產品特性之管理措施。

二、 適用範圍

本文件適用於應用機器學習技術之醫療器材。

三、 人工智慧醫療器材優良機器學習實務之十項原則

1. **應充分理解醫療器材的預期用途/預期目的，並在產品全生命週期中運用多學科專業知識：**深入了解醫療器材的預期用途/預期目的，包括在

臨床工作流程中的使用情境、期望效益及相關患者風險。此舉有助於確保應用機器學習技術的醫療器材，在產品全生命週期內均能滿足具臨床意義的需求。同時，應結合多學科的專業知識，以提供特定情境下的見解與經驗，釐清預期用途/預期目的，並增進器材的安全性與有效性。

2. **在整個產品生命週期中執行良好的軟體工程、醫療器材設計與資訊安全實務：**模型的設計、實施與維護應重視基本要素，包括：穩健的軟體工程實務、可用性(usability)、資料品質保證(data quality assurance)、資料管理、網路安全以及品質管理實務，可參考本署《醫療器材軟體確效指引》[16]、《適用於製造業者之醫療器材網路安全指引》[17]、《醫療器材人因/可用性工程評估指引》[18]。這些實務包括：應執行有系統的風險管理與設計流程，能適當記錄並傳達決策及其理由，同時確保可追溯性（traceability）、再現性（reproducibility）、資料真實性（authenticity）、機密性（confidentiality）、完整性（integrity）與可獲得性（availability）。

應評估醫療實務中全系統安全（total systems safety）的觀點進行風險評估與管理，醫療器材風險管理建議以 ISO 14971 為基礎[4]，並參考人工智慧相關國際標準(如 AAMI TIR 34971、ISO/IEC 23894 等)[5,6]，採用系統層級及使用情境導向之方法，以補強人工智慧相關風險管理。[14] 對模型部署、監測與維護所需的基礎架構亦應進行審慎考量。這些實務有助於維護患者的權利、安全與福祉，亦包括以符合倫理原則的方式使用患者資料，例如依《個人資料保護法》進行資料去識別化處理、取得適當之患者同意等。

3. **臨床評估應使用具有預期病患族群代表性的資料集：**資料收集規範應確保涵蓋預期患者族群之相關特徵（例如年齡、生理性別、族群背景、地理位置、醫療狀況）、預期使用環境以及量測輸入，以確保用於模型訓練、測試與監測的資料集，具備足夠的樣本數與充分代表性，使結果能合理推論至預期的目標族群。對於使用非本土資料集訓練之模型，應評估其於國內族群之適用性及效能差異，並提供相應之資料。前述要求為臨床評估的基本前提，可用於管理任何非預期產生的偏差（unintended bias）或資料漂移（dataset drift，指資料分布隨時間或環境改變），並促進模型在整個預期患者群體中展現出適當且具備泛化能力（generalizable performance）的性能表現，此外也有助於評估器材的可用性，識別模型可能表現不佳的特定情況或子族群（subgroups），並監控這些性能是否會隨時間推移而變化。可參考國際標準進行偏差與資料品質之量測與評估（如 ISO/IEC TR 24027 及 ISO/IEC 5259 系列）[7-12]，以提升模型之準確性與可靠性。若產品係於國內執行臨床試驗者，應符合本署《醫療器材優良臨床試驗管理辦法》[19] 相關規定。
4. **訓練資料集與測試資料集應相互獨立：**訓練與測試資料集的選擇與維護應確保兩者相互獨立。為了確保這種獨立性，應考慮並解決所有可能的潛在相依來源，包括與患者、場域及資料獲取相關的因素。此外，外部驗證（external validation）的程度應與產品的風險成比例。
5. **所選用的參考標準應符合其預期用途：**宜採用臨床及其相關產業領域公認的方法，建立符合預期用途之參考標準（reference standard），以確保所收集之資料具臨床可解釋性且特徵明確，並確保參考標準的局限性（limitation）已被充分理解。具體要求包括：應根據產品預期用

途/預期目的，記錄選擇該參考標準的依據，並評估是否適合預期的使用環境；在模型開發與測試過程中，若有公認的參考標準，應予以採用，以促進並展現模型在預期患者族群中的穩健性和泛化能力；參考標準的選擇應基於廣泛共識（若有）以及適當的專業知識。

6. **應依據可獲得的資料及產品的預期用途/預期目的，選擇與設計模型：**模型的選擇與設計應經過評估，並證明其適用於現有的資料，且能支持主動降低已知風險，例如：過度擬合（overfitting，指模型過於適應訓練資料而降低對新資料之泛化能力）、性能下降（performance degradation）和資訊安全風險（security risks）。此原則的核心要求與考量包括：應充分理解與產品相關的臨床效益與風險，並利用這些資訊來推導出具有臨床意義的性能目標以進行測試，進而支持產品在實現其預期用途/預期目的時的安全性與有效性；在設計與評估模型時，應考慮其對整體預期患者族群以及特定子族群的影響；模型設計應考慮器材輸入、輸出以及臨床使用條件中可能存在的不確定性與變異性（variability）。

7. **產品評估應著重於預期使用環境中的「人-AI 互動」，包括「人-AI 團隊」的協作表現，而非僅評估產品本身：**應在預期使用環境與臨床工作流程的背景下評估產品性能，並在適用情況下考慮與專業醫事人員、患者及照護者之間的互動。此外，應納入人因工程方面的考量，例如：使用者的技能水準與專業知識、使用者對模型輸出及其局限性的理解程度、使用者產生過度依賴的可能性、器材自動化程度，以及在正常使用或可合理預料到使用者可能會做出的錯誤操作，可參考本署《醫療器材人因/可用性工程評估指引》[18]。

評估內容應著重考量，包括但不限於下列項目:

醫事人員之監督責任: 產品設計應考量醫事人員在使用人工智慧時之監督責任，避免自動化偏差陷阱（過度依賴），並確認人工智慧的使用場景與限制確實符合該模型限定的臨床條件與患者需求。

關鍵流程之人為安全評估: 產品設計應考量分析作業流程並定義不可自動化的決策類型與關鍵節點，確保涉及重大醫療決策及醫療行為的環節必須由醫事人員執行。[15]

8. **應在與真實臨床環境相似的條件下進行產品測試：**應制定並執行具有方法學與統計學基礎的測試計畫，以便在獨立於訓練資料集的情況下，產生具備臨床相關性的產品性能資料。在進行測試時，應考量以下因素：預期患者族群及相關的子族群、臨床環境以及「人-AI 團隊」的實際使用情況、量測輸入以及潛在的干擾因素。

9. **應提供使用者清楚且必要的資訊：**應為預期使用者（如專業醫事人員或患者）提供清楚、與情境相關且符合其需求的資訊。這些資訊包含：產品的預期用途/預期目的及適應症、效益及風險；模型在適當的子族群中的性能表現、研究方法學以及用於訓練與測試模型的資料特性（characteristics）；可接受的輸入與已知限制、使用者介面的結果解釋說明、以及模型如何整合至臨床工作流程中，並在可能的情況下提供模型輸出的依據。此外，使用者也應該被告知產品修改（modifications）與更新（updates）的範圍及時程，並獲得可向製造業者溝通產品疑慮的管道。

10. **應持續監控產品在真實環境中的性能，並且管理需要重新訓練之風險：**

已部署的模型應具備在「真實世界（real world）」使用中進行適當程度持續監控的能力，且此監控應以風險為導向，重點在於維持或提升產品的安全與性能，並符合《醫療器材管理法》有關醫療器材變更，以及上市後監督之相關規定。此外，當模型在部署後進行重新訓練時，應有適當的管制措施，以管理可能影響模型安全與性能的風險，例如：過度擬合、非預期偏差或模型劣化（degradation，例如資料漂移）。重新訓練及產品更版部署相關之活動亦應納入醫療器材品質管理系統內實施與管理。品質管理系統之建立與運作應以《醫療器材品質管理系統準則》[20] 為原則，結合 ISO 14971 之風險管理架構。另得參考人工智慧相關國際標準（如 ISO/IEC 42001 等）[13]，建立與既有品質管理系統整合之人工智慧管理機制。業者並應訂定上市後監測計畫，持續追蹤不良事件，並監控真實世界之器材性能，以確保產品於實際使用情境下之安全與性能。

業者得視需求規劃並執行預定變更控制計畫（Predetermined Change Control Plan, PCCP），以管理產品於生命週期中可能發生之變更，可參考本署《應用人工智慧/機器學習技術之醫療器材軟體預定變更控制計畫（Predetermined Change Control Plans, PCCP）申請要點暨撰寫說明指引》[21]。

四、 參考資料

1. IMDRF Artificial Intelligence / Machine Learning Working Group. Good Machine Learning Practice for Medical Device Development: Guiding Principles. IMDRF/AIML WG/N88 FINAL:2025
2. Health Canada, Pre-market guidance for machine learning-enabled medical devices, 2025
3. US FDA, Health Canada, and MHRA, Good Machine Learning Practice for Medical Device Development: Guiding Principles, 2021
4. ISO 14971 :2019 Medical devices — Application of risk management to medical devices
5. AAMI TIR34971:2023 Application of ISO 14971 to machine learning in artificial intelligence—Guide
6. ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management
7. ISO/IEC TR 24027:2021 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making
8. ISO/IEC 5259-1:2024 Artificial intelligence — Data quality for analytics and machine learning (ML), Part 1: Overview, terminology, and examples
9. ISO/IEC 5259-2:2024 Artificial intelligence — Data quality for analytics and machine learning (ML), Part 2: Data quality measures
10. ISO/IEC 5259-3:2024 Artificial intelligence — Data quality for

analytics and machine learning (ML), Part 3: Data quality management requirements and guidelines

11. ISO/IEC 5259-4:2024 Artificial intelligence — Data quality for analytics and machine learning (ML), Part 4: Data quality process framework
12. ISO/IEC 5259-5:2025 Artificial intelligence — Data quality for analytics and machine learning (ML), Part 5: Data quality governance framework
13. ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system
14. ECRI, Managing the Risks of AI in Healthcare, 2025
15. ECRI, Ethical Use of AI in Healthcare, 2024
16. 醫療器材軟體確效指引,FDA 器字第 1061607211 號公告,106 年 12 月 15 日
17. 適用於製造業者之醫療器材網路安全指引，FDA 器字第 1101603391 號公告，110 年 5 月 3 日
18. 醫療器材人因/可用性工程評估指引，FDA 器字第 109160117 號公告，109 年 4 月 13 日
19. 醫療器材優良臨床試驗管理辦法，110 年 04 月 09 日
20. 醫療器材品質管理系統準則，110 年 04 月 14 日
21. 應用人工智慧/機器學習技術之醫療器材軟體預定變 更控制計畫(Predetermined Change Control Plans, PCCP)申請要點暨撰寫說明指引，FDA 器字第 1131607731 號公告，113 年 9 月 23 日