

新光醫療財團法人新光吳火獅紀念醫院院內外資料治理管理辦法

民國 115 年 08 月 28 日制定

管理單位：資訊部、數位醫學部數位資訊科

- 第 1 條 新光醫療財團法人新光吳火獅紀念醫院（以下簡稱本院）為規範院內資料、院外資料及廠商平台或設備（含物聯網醫療設備，Internet of Medical Things, IoMT）之申請、審查、去識別化、串接、驗證、上傳、建置、上架及管理流程，確保資料使用符合法令規範、資訊安全、臨床治理、系統整合及資料品質要求，並維護本院病人權益、醫療資訊系統穩定性與資料治理秩序，特訂定「院內外資料治理管理辦法」（以下簡稱本辦法）。
- 第 2 條 本辦法適用對象如下：
- 一、本院各單位申請使用、介接、匯入、交換、分析、建置或上架院內外資料之人員。
 - 二、申請導入院外資料、第三方平台、雲端服務或 IoMT 設備之本院人員、合作單位及專案承辦人。
 - 三、配合本院辦理資料介接、系統整合、資料驗證、測試、維運、建置或治理相關作業之廠商。
 - 四、負責院內原始資料管理、去識別化、排程上傳、資料平台建置及後續管理之權責單位與人員。
- 第 3 條 本辦法所稱院內外資料治理，係指對資料來源、蒐集方式、使用目的、資料最小必要原則、權限管理、去識別化、介接方式、資料品質、資訊安全、法規遵循、驗證程序、平台上架及後續管理等事項所進行之審查與管理；其範圍包括院內既有資料、院外合作資料、廠商平台資料、醫療儀器或 IoMT 設備產出資料，以及其他經本院認定應納入治理之資料。
- 第 4 條 本院院內原始資料由資訊部統一管理。院內資料如有提供分析、治理、整合、研究、決策支援或平台建置之需要，原則應先於院內完成去識別化處理後，始得依核准流程上傳至本院指定之資料管理平台或其他經核准之平台。
- 第 5 條 現行院內資料上傳至資料管理平台者，以本院相關資料庫為原則。資訊部得依系統特性、資料敏感性、臨床需求、平台容量、維運資源及治理條件，訂定資料上傳範圍、頻率、方式及相關控管措施，並以排程方式辦理資料上傳作業。
- 第 6 條 除前條所定資料庫外，如其他單位提出新增院內資料庫建置、資料集上傳或主題資料區建置需求，應先向資訊部諮詢其必要性、可行性及資料來源適切性。初次諮詢通過後，申請單位始得提報臨床治理小組審查；經審查通過者，由資訊部依核准範圍辦理相關資料表上傳，並由數位醫學部數位資訊科於資料管理平台進行後續建置、整理、管理及維護。
- 第 7 條 院內資料上傳、建置及管理作業，應遵循下列原則：
- 一、原始資料管理權責屬資訊部；未經核准，不得自行擷取、複製、搬移或另行建置原始資料庫。
 - 二、資料提供前應確認去識別化、欄位定義、更新頻率及使用目的，並避免超出核准範圍之資料暴露。
 - 三、資料管理平台之資料模型、主題資料區、權限設定與後續管理，由數位醫學部數位資訊科依核准內容辦理。
 - 四、如涉及跨系統串接、跨單位共享或高敏感資料，必要時得再提臨床治理小組或相關權責單位確認。

- 第 8 條 院外資料或廠商平台、IoMT 設備擬導入本院前，申請人應先提出申請，並檢附必要文件及說明資料。前項文件及說明，原則應包括下列內容：
- 一、申請目的、使用情境、預期效益及需求說明。
 - 二、資料來源、資料欄位、更新頻率、保存方式及資料流向說明。
 - 三、平台或設備之功能說明、系統架構、網路架構及部署方式。
 - 四、資料介接方式、通訊協定、API 規格、交換標準或設備輸出格式等技術文件。
 - 五、資訊安全機制、帳號權限管理、傳輸加密、存取控制、日誌紀錄及異常通報機制。
 - 六、個人資料、敏感資料、醫療資料或其他依法應受保護資料之處理方式。
 - 七、其他經資訊部門、臨床治理小組或本院要求補充之資料。
- 第 9 條 院外資料導入、廠商平台或 IoMT 設備介接申請案件，應先送資訊部辦理初步審核及資安審查；未完成前項審查者，不得逕行介接、測試、交換或匯入資料。資訊部辦理審查時，應就下列事項進行評估：
- 一、申請內容是否完整，申請目的是否明確且具必要性。
 - 二、資料來源及介接方式是否符合本院資訊架構與管理原則。
 - 三、廠商、平台或設備之資訊安全管理制度是否具備適當證明文件，並優先確認是否通過相關資安認證，如 ISO 27001，或其他經本院認可之等同性資安標準。
 - 四、是否涉及個人資料、病歷資料、敏感性資料或跨機構資料傳輸之風險。
 - 五、是否有影響本院既有系統穩定性、網路安全或資料品質之虞。
- 第 10 條 經資訊部初步審核同意之院外資料、廠商平台或 IoMT 導入案件，應提報臨床治理小組審議。申請人應於會議中說明平台、設備或資料之臨床應用情境、資料內容、介接目的及導入後擬如何串接進本院醫療資訊系統。臨床治理小組得依案件性質，就其臨床必要性、病人安全、資料合理性、作業流程改變、權責分工及治理需求進行審查。
- 第 11 條 案件經臨床治理小組審議通過後，由資訊部提供申請案件單號，並就技術細節、執行方式、系統影響與資源需求進行評估。其評估事項，原則包括下列內容：
- 一、資料格式、欄位定義、編碼規則及標準化程度。
 - 二、介接方式、交換機制、測試環境需求及與既有系統之整合可行性。
 - 三、資料傳輸安全、身分驗證、權限控管、憑證管理及稽核追蹤機制。
 - 四、系統效能、穩定性、維運責任、異常處理及備援機制。
 - 五、資料寫入、更新、回補、清理或停用機制。
- 第 12 條 申請人應依資訊部之要求，配合辦理資料驗證及測試作業。前項資料驗證，至少應確認資料之正確性、完整性、一致性、可用性及與原始來源之一致情形；必要時，並應提出驗證報告、測試紀錄或其他可供審查之佐證文件。未完成驗證或驗證結果不符要求者，不得進入正式上線或平台上架階段。
- 第 13 條 案件經評估具執行可行性，且資料驗證結果符合要求者，得依資料性質、使用目的、權限設計、保存需求及治理要求，決定是否上架至本院指定之資料平台或其他經核准之資料平台。前項上架與否，應由資訊部會同相關權責單位審酌後決定，必要時得再提臨床治理小組確認。
- 第 14 條 資料或設備完成導入、介接、上傳、建置或平台上架後，申請單位相關單位應持續辦理下列治理事項：
- 一、資料權限管理、帳號管理及最小必要使用原則之落實。
 - 二、資料品質監控、異常值檢核、更新頻率確認及版本管理。

- 三、去識別化規則、資料流向、存取紀錄及稽核軌跡之保存。
- 四、資安事件、資料外洩、設備異常或系統故障之通報及處理。
- 五、委外廠商、合作單位或平台提供者之持續管理及合約遵循事項。
- 六、法令、政策、院內規範或臨床治理要求變更時之調整作業。
- 第 15 條 申請人、使用人員、管理單位及廠商，均應遵守本院資訊安全、個人資料保護、醫療資料管理、研究倫理及其他相關規定，不得有下列情形：
- 一、未經核准即擅自介接、匯入、交換、複製、下載、提供、上傳或使用資料。
- 二、規避審查程序、資安管制、去識別化要求、權限管理或稽核機制。
- 三、提供不實文件、隱匿重要資訊或未依核准範圍使用資料。
- 四、將資料或系統存取權限轉供他人使用，或使未經授權之第三人得以接觸資料。
- 五、其他足以影響本院病人權益、資訊安全、系統穩定或資料治理秩序之行為。
- 第 16 條 違反本辦法者，依其情節輕重，得採取下列處理方式：
- 一、停止案件申請、測試、介接、上線、平台上架、資料建置或資料使用。
- 二、停止或限制相關帳號、設備、平台、系統或資料之使用權限。
- 三、要求限期改善、補正文件、重新驗證或重新提報審查。
- 四、依本院相關規定辦理責任釐清、行政處置、合約處理或其他必要措施。
- 五、如涉及法令違反、個資外洩、資安事件或其他重大情事者，應依相關規定通報並辦理後續處置。
- 第 17 條 本辦法授權各權責單位得依業務需要訂定相關申請流程、標準作業程序等規範，本辦法如有未盡事宜，悉依相關法令、本院資訊安全規定、個人資料保護規範、醫療資訊系統管理規範、資料平台管理原則及其他相關制度辦理。
- 第 18 條 本辦法如有修正或廢止時，經臨床治理小組審議通過，陳院長核准後公告實施。

附件一、院外資料／廠商 IoMT 導入院內流程圖

(申請、資安審查、臨床治理審查、技術評估、資料驗證及資料平台上架流程)

院外資料 / 廠商IoMT導入院內流程圖

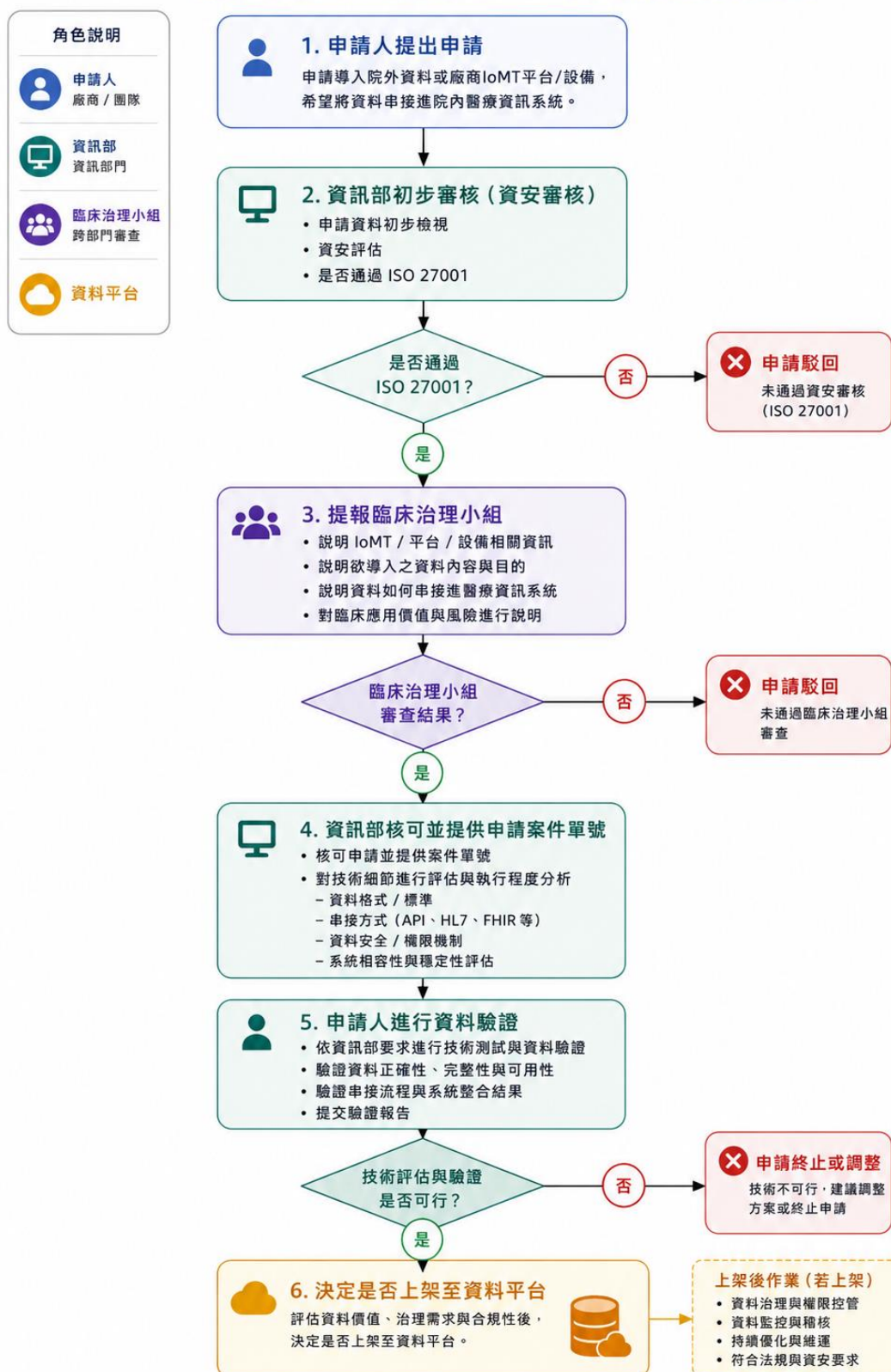


圖 1 院外資料／廠商平台或設備（IoMT）導入院內流程圖

附件二、院內資料管理流程圖

(院內原始資料管理、去識別化、上傳與資料平台建置流程)

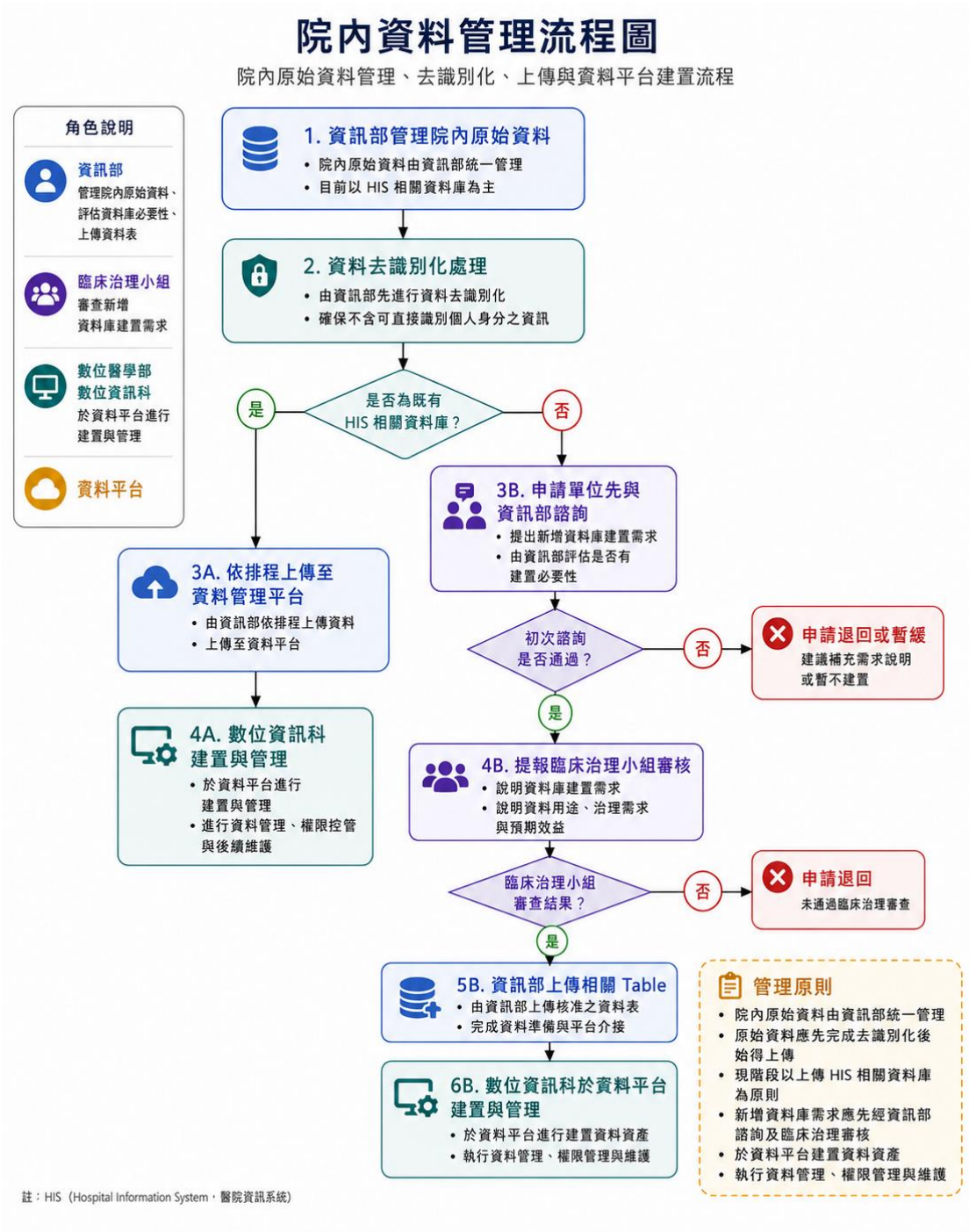


圖 2 院內資料管理流程圖