馬偕紀念醫院
MacKay Memorial Hospital

ISO27701 個人資料安全驗證及顧問輔導服務案

規格說明書

2025 年 10 月 21 日

壹、 服務對象

一、台灣基督長老教會馬偕醫療財團法人馬偕紀念醫院（以下簡稱台北馬偕）。

二、台灣基督長老教會馬偕醫療財團法人淡水馬偕紀念醫院（以下簡稱淡水馬偕）。

三、台灣基督長老教會馬偕醫療財團法人台東馬偕紀念醫院（以下簡稱台東馬偕）。

四、台灣基督長老教會馬偕醫療財團法人新竹馬偕紀念醫院（以下簡稱新竹馬偕）。

五、台灣基督長老教會馬偕醫療財團法人馬偕兒童醫院（以下簡稱兒童醫院）。

六、新竹市立馬偕兒童醫院(委託台灣基督長老教會馬偕醫療財團法人興建經營，以下簡稱新竹馬偕兒童醫院)。

貳、 專案範圍

一、協助資訊單位提供之資訊安全管理活動，涵蓋醫療資訊系統、醫療影像系統、健保醫療資訊雲端查詢系統批次下載、電子病歷系統之開發、維護管理，及其相關之電腦機房實體安全、網路安全管理、醫事單位提供之醫務管理業務、病歷資料管理作業、病歷存放實體安全、掛號批價作業、健保申報業務、人事單位提供之 HCA 醫事憑證管理中心醫事人員行動憑證管理服務窗口作業（RAO）、遠距照護服務提供之遠距醫療作業（通訊診察治療辦法），導入 ISO 27701：2019 隱私資訊管理系統驗證且取得經我國標準法主管機關委託機構之公正第三方驗證，於合約有效期間維持 ISO 27701：2019 證書

之有效性及顧問輔導服務。

二、指導本院執行「醫院個人資料檔案安全維護計畫」之要求並建立相關個資保護程序。

三、為 ISO/IEC 27701：2019 轉版進行相關準備。

參、 專案期間

自 115 年 01 月 01 日起至 116 年 12 月 31 日止，共二年。

肆、 工作內容

依照 ISO 標準所述流程的精神，廠商應將輔導活動細分成：需求分析及個人資料之範圍及項目建立、文件修訂維護、制度規範宣導及檢核等，同時以專案管理的精神，管控所有活動的進行，確保專案能如期如質地完成。

一. 配合本院之資訊安全管理系統(ISMS)建立/調整個人資料保護管理系統(PIMS)之四階文件：交付管理程序書及表單(適用於 ISO27701:2019 年版)

二. 個資盤點作業：協助本院(台北馬偕、兒童醫院、淡水馬偕、台東馬偕、新竹馬偕、新竹馬偕兒童醫院)進行個資之盤點、個資風險評鑑作業，並交付個資清冊、風險評鑑報告、風險處理計畫等。

三. 實作個資管理制度：提供定期或不定期個人資料保護管理系統顧問諮詢輔導服務。

四. 個資事故演練管理：廠商需指導驗證範圍內之單位執行個資事故應變演練活動。

五. 個資保護內部稽核：

(一)每年應依據「醫院個人資料檔案安全維護計畫」進行兩次內部稽核，包括(台北馬偕、兒童醫院、淡水馬偕、台東馬偕、新竹馬偕、新竹馬偕兒童醫院)，且符合「個人資料保護法」

及其子法等相關法規以及 ISO/IEC 27701:2019 隱私資訊管理系統證書驗證範圍，應於稽核前交付稽核計畫，稽核完成後交付稽核報告、以及協助提供稽核後缺失之持續改善措施之建議。

(二)廠商擔任稽核之人員，須具有 ISO/IEC 27001:2022 Information Security Management Systems(ISMS) Auditor/ Lead Auditor 資通安全專業證照、ISO/IEC 27001:2019 Privacy Information Management System （PIMS）Auditor/Lead Auditor 隱私資訊安全專業證照

六. 管理審查：廠商須配合本院於合約有效期間指導院方準備管理審查會議資料，並安排專案人員 1 名出席該會議。

七. 第三方驗證協助：

(一)廠商需依據院方個人資料保護管理系統驗證範圍，安排驗證機構進行年度稽核，以協助本院維持 ISO/IEC 27701:2019 證書之有效性。

(二)廠商需於驗證機構執行稽核前，協助院方準備驗證機構稽核所需相關文件。

(三)廠商應於外部驗證其間，安排顧問在場進行協助院方通過稽核。

(四)依據驗證機構稽核結果所提出之相關不符合事項，提供改善措施之規劃與執行建議，並符合「MMH-ISMS-2-GE-007 改善措施管理規範」規定。

八、 廠商選擇之驗證機構及驗證文件應持續有效，且驗證文件之發證單位應為國際論壇（International Accreditation Fourum，IAF）認證機

構認可之驗證機構。

伍、 專案管理需求

一.專案管理

得標廠商應就本專案之規劃管理、組織、時程及進度查核等方面撰寫專案執行計畫書，內容應包含專案規劃及執行方式說明、專案管理、專案組織、人力配置、交付項目、專案時程及進度查核、工作對應窗口、專案驗收及本院配合事項等。

二、專案組織與人力

(一)得標廠商應研擬評估預計投入本專案之人員配置與資歷（學經歷背景與技術專長)。參與本專案之專案成員需 2 人以上，且為承包廠商連續在職 1 年以上之全職員工，並依各項服務需求所要求具備之證照，於專案執行計畫書中提出相關證明，於專案執行計畫書中提出相關證明，並填具委外廠商專案人員資格審查表(附件一)。專案團隊至少需持有下列證照一張或以上。

1. 須具有 ISO/IEC 27001:2022 Information Security Management Systems(ISMS) Auditor/ Lead Auditor。
2. ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor。

(二)本院有權要求更換專案成員，得標廠商應於接獲本院通知後 1 個月內完成更換。

(三)得標廠商於專案執行計畫書提出之專案組織與人員應與實際執行本專案之人員相符，得標廠商若欲異動專案成員須於 1 個月前通知本院，並經本院同意後始可異動。

三. 廠商投標資格

(一)具輔導醫療機構通過 ISO/IEC 27701:2019 驗證經驗尤佳。

(二)需政府機關登記合格，無不良紀錄之廠商（檢附設立及登記證明、納稅證明及信用證明）且不得為陸資企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。本案服務人員需具有中華民國國籍，不得為外籍勞工或大陸來台人士。

四. 安全需求

(一)得標廠商參與本案之專案人員進行本案之相關專案工作時，應注意資訊安全之防護措施，須依照本院規定簽訂保密切結書（詳附件二）及馬偕醫療財團法人體系合作廠商保密同意書（詳附件三），並確實要求所屬人員遵守保密規定，倘經發現因前述事由而洩密者，一切損害由得標廠商負責，並依法追究刑事責任。

(二)得標廠商參與本案之專案人員因工作之便所接觸之資料不得私自進行留存、備份、篡改或販售等行為，如因疏失造成本院各項資訊作業與文件資料之毀損與損失，由得標廠商負責賠償責任，本院並保留損失估計權利。廠商使用之資通訊工具需符合國家安全規定。

(三)得標廠商須將本院委外契約共同條款表（詳附件四）簽訂於合約規範中，並確實要求所屬人員遵守規定。

五. 強制性需求

(一)本專案於合約期間內所取得之資料，於本專案合約終止後應完整歸還，不得複製。

(二)第三方驗證協助之驗證機構稽核報告其驗證結果若為無效，其缺失改善再複驗所產生之費用，將由得標廠商負擔。

(三)得標廠商未依本專案合約履行者，本院得解除或終止合約。

(四)得標廠商於簽約時須同時簽訂保密與責任條款。

陸、 附件

（一） 馬偕紀念醫院委外廠商專案人員資格審查表

（二） 馬偕紀念醫院人員保密切結書

（三） 馬偕醫療財團法人體系合作廠商保密同意書

（四） 馬偕紀念醫院委外契約共同條款表