

108 年人體生物資料庫查核作業說明會問答集

一、人體生物資料庫查核程序及制度

序號	內容
1	Q：是否建議人體生物資料庫進行ISO27001認證？ A：本年度未要求人體生物資料庫須參加ISO27001之認證，各人體生物資料庫可自行評估是否參加；惟機構有通過ISO27001認證，且認證範圍包含人體生物資料庫資訊系統，於查核時可提供相關佐證資料。

二、人體生物資料庫查核基準及評量項目

序號	內容
1	Q：基準2.1「設置倫理委員會，委員組成符合法令規定，會務運作正常並有委員教育訓練」，註第2點「教育訓練課程可併倫理委員會議辦理」，會議時間及課程時間可以加總在一起為教育訓練時數嗎？ A：訓練課程可併倫理委員會議辦理，係指人體生物資料庫可利用EGC會議時間（或會議前、會議中或會議後）安排教育訓練課程，惟時數計算應僅能計算實際進行課程時間，不應包含會議時間。
2	Q：基準4.2「生物檢體建檔編碼時，已去辨識化且可辨識個人資料之保存規範」，有關人體生物資料庫解密權限，委員建議應有2位主管以不同金鑰同時輸入才可再連結個資，請問主管資格認定？ A：資料解密作業為確保資訊安全，不應僅有1人擁有金鑰即可回復資料，至少應有2位不同人員同時操作方可回復；惟人員之資格由人體生物資料庫依其作業程序規定辦理。
3	Q：基準4.4「人體生物資料庫系統應有定期實施弱點掃描並提供完整弱點掃描報告及相關紀錄」，應執行弱點掃描之資訊系統是只有處理個資的系統還是包含所有資料的系統？ A：除已實體隔離網路之資訊系統，人體生物資料庫中所有可連接網路之資訊系統皆應執行弱點掃描。

序號	內容
4	Q：基準5.2「應取得參與者同意書，並有相關保存及管理機制」，符合項目2「參與者同意書簽署之完整性及適切性」之定義？ A：參與者同意書完整性係指應簽署欄位之簽署完整性，包含參與者/法定代理人之資料、簽名及日期；適切性則為參與者同意書取得過程之適切性。