110年度人體生物資料庫教育訓練

實體與資料的管理，不同類型的資料處理方式與識別

林口長庚紀念醫院 臨床試驗中心 傅昶叡

大綱

- 人體生物資料庫 資訊管理系統
- 人體生物資料庫 個資管制流程
- 人體生物資料庫 資訊安全管理
- 管理面上的議題分享

人體生物資料庫 資訊管理系統

人體生物資料庫的資訊系統類型

收案人員 網路管制環境	資訊組 網路管制環境	生物醫學組 內部網路環境	專案管理 內部網路環境	線上使用者 外部網路環境
參與者 收案管理	資料收集管理 及分類	生物檢體庫 物流管理	合作專案	生物資料庫 研究案例查 詢系統
參與者 個資管理	資料去識別 管理	實驗室作業 管理	申請案件 管理審查	生物研究資 料回饋系統
	跨系統資料 交換管理		資料輸出 案件追蹤	

人體生物資料庫 - 收案作業環境

參與者收案管理系統

- 參與者聯繫窗口
- 參與者同意內容管理
- 參與者異常事件管理
- 參與者溝通管理

參與者個資管理系統

- 參與者同意書檔案管理
- 參與者個資保護
- 參與者基本資料管理
- 原始資料檔案管理

人體生物資料庫 – 資訊組作業環境

資料收集管理及分類

- 資料收集、管理檢核
- 個案族群分類
- 整合醫療資訊及其他系統資訊
- 資料標準化作業
- 研究者回饋資料管理

資料去識別管理

- 資料去識別管理
  - 外部收集資料去識別
  - 再識別管理流程 (解盲)
- 內部作業資料去識別管理
  - 檢體、衍生物、實驗資料
- 外部申請資料去連結管理
  - 外部申請資料獨立去連結
- 去識別資料疑義處理
  - 申請方資料問題反映及釐清

跨系統資料交換管理

- 人體生物資料庫整合平台
- 資料標準化轉換
- 資料交換管制作業

人體生物資料庫 - 生物醫學組作業環境

生物檢體庫物流管理

- 生物安全性管理
- 貯存環境管理
- 檢體物流紀錄
- 檢體品管紀錄
- 檢體異常事件紀錄
  - 歷史溫度

實驗室作業管理

- 衍生物製作及品管作業
- 檢體實驗室操作
- 檢體實驗記錄資料建檔
- 生物資訊建檔
- 生物資訊分析建檔

人體生物資料庫 – 專案管理 及 線上使用者

專案管理系統

- 各類合作專案管理
  - 特殊合作案件收案管理
  - 異常事件管理
- 申請案件管理審查
  - 科學審查
  - 倫理委員會審查
- 輸出案件後續追蹤
  - 檢體使用情況追蹤
  - 研究資料回饋追蹤
  - 研究成果追蹤
  - 商業利益追蹤
  - 申請者異常事件追蹤

線上查詢、申請及資料回饋

- 生物資料庫研究案例查詢
  - 結構化篩選條件查詢
  - 生物資料申請進度查詢
- 生物研究資料回饋系統
  - 生物資料使用狀況回報
  - 實驗結果線上回饋
  - 實驗資料檔案批次上傳
  - 研究檢體異常事件反映

人體生物資料庫 個資管制流程

個人資料定義

個人資料保護法 (2015/12/30)

第二條 第一項

個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

歐盟 GDPR (2018/5/25)

- 個人身分、生物特徵
  - 例如電話號碼、地址、車牌、病歷資料、指紋、臉部辨識、視網膜掃描、相片、影片、電郵內容、問卷表單等，甚至社會認同、文化認同、地理位置等，只要是一個人所能產生出的任何資料，幾乎都被重新定義為個人資料並受到保護。
- 線上定位資料
  - 例如 Cookie、IP 位置、行動裝置 ID、社群網站活動紀錄等。

個人資料組成

- 社會資訊
  - 社會識別資訊：不變或少變且可連結個體的資訊
    - 姓名、國民身分證統一編號、護照號碼、病歷號碼
    - 綽號、網路帳號等廣為人知的假名
    - 其他得以直接或間接方式識別該個人之資料
    - 不一定具有唯一性，不一定具備恆常的連結性
  - 社會活動紀錄：隨時間變動的個體社會狀態紀錄
    - 學歷、經歷、就業狀態、財務狀態、婚姻狀態
    - 各類文字、照片、影像紀錄等
    - 醫療、性生活、健康檢查、犯罪前科、聯絡方式
- 生物資訊
  - 生物識別資訊：不變或少變且可連結個體的資訊
    - DNA、指紋、聲紋、視網膜、靜脈分布
    - 具備唯一性與恆常的連結性
  - 生物特徵資訊：不變或少變的外顯分類資訊
    - 種族、性別、瞳孔顏色、長相
  - 生物動態資訊：隨時間變動的生理狀態
    - 病歷、健康狀況、體溫、血壓、身高、體重
    - 檢驗檢查紀錄、基因以外的分子生物資

- 任何資料跟社會識別資訊有所連結就算個人資料?
  - 是否具備敏感性，是否會傷害其社會權益
  - 公共利益間的衝突
- 任何類型資訊均可透過相互串聯及資訊累積來提高特異性，達到間接識別個體的目的
  - 是否與社會識別資訊有直接連結
  - 資料精細度、資料多樣化程度、資料累積量

生物醫學研究的個人資料保護

- 個資法 第六條

  有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

  四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

- 施行細則第三條
  - 得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。
- 施行細則第十七條
  - 無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。

去識別 (Anonymization)

目的：無從識別特定當事人

敏感資料必須除去以下的特性

- 標定性 (singling out)
- 連結性 (linkability)
- 推論性 (inference)

假名化(pseudonymization)
- 算不算完整的去識別?
- 替代編碼、加密編碼

從而，保護當事人的社會權益及尊嚴
- 與公共利益間有衝突時?

- 疫調足跡
  - 敏感資料
    - 確診資訊、出入場所、爭議行為
  - **連結性：上下的資料產生關連**
  - 標定性
    - 案例編號、個人基本資料
  - 推論性
    - 組織、群體 → 特定族群負面形象
    - 在組織的職稱、居住地區、年齡、嗜好 → 可能推論出個人識別

去連結、去識別相關定義

- 人體研究法 第四條
  - 去連結：指將研究對象之人體檢體、自然人資料及其他有關之資料、資訊（以下簡稱研究材料）編碼或以其他方式處理後，使其與可供辨識研究對象之個人資料、資訊，永久不能以任何方式連結、比對之作業。
- 人體生物資料庫管理條例 第三條 第五、六、七項
  - 五、編碼：指以代碼取代參與者姓名、國民身分證統一編號、病歷號等可供辨識之個人資訊，使達到難以辨識個人身分之作業方式。
  - 六、加密：指將足以辨識參與者個人身分之資料、訊息，轉化為無可辨識之過程。
  - 七、去連結：指於生物檢體、資料、資訊編碼後，使其與可供辨識參與者之個人資料、資訊，永久無法以任何方式連結、比對之作業。
- 人體生物資料庫管理條例 第十八條 第一項
  - 設置者就其所有之生物檢體及相關資料、資訊為儲存、運用、揭露時，應以編碼、加密、去連結或其他無法辨識參與者身分之方式為之。

  → **假名化**
- “假名化”或“去識別”仍允許另外保存個資的連結性，但管制其使用

個資管理系統功能

- 去識別
  - 對象：人體生物資料庫內部人員
  - 目的：避免人體生物資料庫人員探知檢體提供者身分
  - 處理方式：替代索引欄位(系統唯一性編碼)、刪除欄位、降低資料精確度
- 去連結
  - 對象：人體生物資料申請者
  - 目的：除去識別以外，限制申請者所取得人體生物資料僅能使用於該次申請範圍，避免申請者透過多次申請累積私人資料庫
  - 處理方式：替代索引欄位(申請案唯一性編碼)

個資管理系統功能

- 再識別
  - 對象：稽核人員、
  - 目的：定期稽核、知情同意書調閱、異常事件追溯等
  - 處理方式：個資管制室調閱對應資料
- 資料更新，追加欄位
  - 對象：人體生物資料申請者
  - 目的：原申請生物資料範圍內之附加資料更新(如檢體提供者存活狀態)或追加欄位等
  - 處理方式：個資管制室調閱對應資料後，依原申請案編碼提供資料更新

個資管制系統：去識別

- 目的
  - 管理條例第12條：採集、處理、儲存或使用生物檢體之人員，不得洩漏因業務而知悉或持有參與者之秘密或其他個人資料、資訊。
  - 去除任何追溯檢體提供者身分之可能
  - 確保資料可用性
- 處理方式
  - 可追溯身分欄位
    - 直接資料：身分證號、姓名、生日、各類聯絡方式、家屬或照顧者個資
    - 間接資料：外部含個資資訊系統的各類索引，如病歷號、門診號、處方單號
- 處理方式(續)
  - ...若可用於資料分析
    - 降低精確度
    - 採用其他分類
  - ...若為資料檢索必須欄位
    - 新替代性索引或新資料關聯
    - 索引代碼的唯一性範疇為**整個人體生物資料庫**
  - **...其他一律刪除**

個資管制系統：去識別

- 知情同意書
  - 標的欄位：參與者身分代碼、歸戶代碼
  - 處理方式：僅保留知情同意書編號或系統代碼索引
- 檢體提供者基本資料
  - 標的欄位及處理方式：
    - 身分證號 → 採用替代代碼或加密代碼識別
    - 生日 → 精確度降至年月
    - 地址 → 精確度降至鄉鎮區
    - 電話 → 刪除
    - Email → 刪除
- 檢體來源單位作業資料及外部來源資料
  - 標的欄位：原單位/計劃案之各資料表索引主鍵
  - 處理方式：建立新索引主鍵取代原索引主鍵，由個資管制室保管原始對應

個資管制系統：去連結

- 目的
  - 避免申請者用任何其他途徑重新識別參與者身分
  - 確保資料僅適用於所申請範圍用途
  - 不同申請案所取得資料的彙整難度高
  - 避免申請者累積私庫
- 處理方式
  - 同去識別處理模式，但所有替代索引代碼唯一性範疇縮小至申請案。
    - **A申請案的S001個案與B申請案的S001個案不會是相同個案**
  - 替代索引代碼與原識別代碼的對應由個資管制室管制，以作為資料更新的依據，但**不得作為資料申請者重新識別檢體提供者身分之用途**(人體生物資料庫管理條例第三條用詞定義)。

個資管制系統：再識別/資料更新或追加

- 目的
  - 參與者退出時相關資料的銷毀
  - 因稽核目的需追溯檢體提供者身分時
  - 異常事件追蹤(如感染性檢體)
  - 外部資料來源端資料異動或訂正，須更新生物資料庫資料者
- 處理方式
  - 由個資管制室對所查詢檢體或個案，解密檔案檢體提供者身分
  - 依照檢體提供者身分，調集所需資料或原始文件
  - 資料如需提供生物資料庫人員閱覽，需再經去識別程序方得為之
  - 資料如需交付予申請者，需再經去連結程序方得為之

個資管制系統：整合外部資料庫

- 新檢體入庫：
  - 個資管制室進行參與者建檔之後，整理新參與者列表向外部資料源求取**完整資料**
- 已在庫檢體：
  - 個資管制室定期彙整參與者列表及最後更新日期資訊，向外部資料源求取**應更新資料**
- 個資管制室將已取得資料歸戶匯入含個資整合資料庫中，並產生去識別代用欄位
- 個資管制室準備去識別匯出檔，將所有識別資訊刪除後，交予生物資料庫管理系統匯入資料
- 進行資料庫備份作業

個資管制系統：生物資料查詢、申請與輸出

- 資料篩選查詢
  - 申請案目標族群
    - 整合愈多的資料來源，篩選條件可以更精細，有助提升研究品質
    - 減少檢體的浪費
  - 檢體類型、狀態
    - 包含檢體類型、儲存溫度、以及過往異常事件歷程
- 申請範圍之資料備置
  - 針對適用的個案及檢體，提供申請範圍內的資料欄位
  - 去識別且去連結
  - 必須確保在替換索引值後，多檔案間的索引關聯仍可正確連結，避免因不當的加密導致無法串檔
  - 執行的資料庫操作程式碼得有第二人檢查且應保留存查。
  - 出庫前抽樣QC

人體生物資料庫 資訊安全管理

人體生物資料庫
資訊安全管理 與 ISO/IEC 27001:2013對應

- 資訊管理單位之組織、權責及分工
- 人員管理
- 電腦系統安全管理
- 網路安全管理及通訊管理
- 資訊系統存取控制管理
- 資訊系統購置、發展及維護安全管理
- 資訊資產之管理
- 實體及環境安全管理
- 業務持續及回復管理
- 密碼管理、電子簽章及資料加解密管理
- 個人資料管理及去識別管理
- 其他相關資訊安全事項
- 倫理委員會審查

資訊管理單位之組織、權責及分工

審查要項

1. 訂有負責資訊安全管理事項之協調、推動、辦理資訊安全政策、規劃、執行等審議、督導事項之人員或推行小組。

ISO/IEC 27001:2013對應

A.6 資訊安全組織

- 內部組織：資訊安全角色及責任、職務區隔、主管機關之聯繫、外部機構之聯繫、專案管理

人員管理

審查要項

2. 訂有人員管理相關規定及程序，且內容至少須包含以下事項：
   - A. 人員安全評估
   - B. 設置者、使用生物檢體及相關資料、資訊之第三人，其資訊管理人員與研究人員不得互為兼任之說明
   - C. 生物檢體其相關資料、資訊之資訊硬體系統與生物檢體本身，應分別指定專人管理；且該專人不得兼任資訊管理人員之說明
   - D. 人員離（休）職之必要手續（含立即取消使用各項資訊資源之所有權限）

ISO/IEC 27001:2013對應

- A.7 人力資源安全
  (1) 聘用前：篩選程序、聘用條款條件
  (2) 聘用期間：管理階層責任、資訊安全認知及教育訓練、獎懲規定
  (3) 聘用之終止及變更

電腦系統安全管理

審查要項

3. 訂有電腦系統安全管理規定，且內容至少須包含以下事項：
   - A. 針對使用者電腦訂定軟體安裝管控規則
   - B. 定期確認授權軟體及免費軟體之使用情形
   - C. 定期更新漏洞、電腦病毒碼及其他惡意軟體防範程式
   - D. 針對個人行動裝置及可攜式媒體訂定管理程序
   - E. 針對全部資通系統定期辦理網站安全弱點檢測

4. 訂有資通系統及相關設備監控措施 (如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等)，且針對日誌建立適當之保護機制，以避免遭到竄改。

電腦系統安全管理

ISO/IEC 27001:2013對應

- A.12 運作安全
  (1) 作業程序及責任：文件審查、變更管理、容量管理、開發測試及運作環境之區隔
  (2) 惡意軟體防範
  (3) 備份備援
  (4) 事件紀錄及監控
  (5) 運作中軟體之監控
  (6) 系統弱點管理
  (7) 稽核影響

網路安全管理及通訊管理

審查要項

5. 訂有參與者之個人資料，以實體隔離之方式建構及使用，且其資訊系統不得與網際網路連接。

6. 訂有人體生物資料庫有關資訊，非經設置者倫理委員會認可之技術加以處理，不得以電子郵件或其他電子方式對外傳送；且經倫理委員會認定有特別保密必要之機密文件，不得以電子方式傳輸。

7. 訂有網路服務安全控制措施，且內容至少須包含以下事項：
   - A. 網路分隔控制規定
   - B. 遠端連線使用者之存取須身分鑑別
   - C. 無線網路服務之存取及應用訂有安全管控程序

8. 訂有定期檢測網路運作環境之安全漏洞機制

9. 訂有網路監控措施，且針對日誌建立適當之保護機制，以避免遭到竄改

網路安全管理及通訊管理

ISO/IEC 27001:2013對應

- A.13 通訊安全

  (1) 網路安全管理：網路控制措施、網路服務之安全、網路之區隔

  (2) 資訊傳送：資訊傳送政策及程序、資訊傳送協議管理、電子傳送安全性、機密性及保密協議

資訊系統存取控制管理

審查要項

10. 訂有系統存取政策及授權規定及程序，且內容至少須包含以下事項：
  - A. 系統存取政策及授權規定經倫理委員會審查通過後，以書面、電子或其他方式告知員工及使用者相關之權限及責任。
  - B. 人員之系統存取權限，以執行其職務所必要者為限。
  - C. 系統管理最高權限之人員及掌理重要技術及作業控制之特定人員審慎授權。
  - D. 系統管理最高權限之人員至少應有二人。
  - E. 系統使用者註冊管理機制。
  - F. 使用者之密碼長度及複雜度規定。
  - G. 依運用系統及安全管理需求訂定密碼周期，且最長以六個月為限。
  - H. 針對系統存取特別權限之人員建立使用人員名冊，並加強安全控管及縮短通行密碼更新周期。
  - I. 資訊存取紀錄應保留一定時間，並限制紀錄之存取活動規定。

資訊系統存取控制管理

ISO/IEC 27001:2013對應

- A.9 存取控制

  (1) 存取控制規定：存取控制政策、網路服務存取

  (2) 使用者存取管理審查：使用者註冊及註銷、使用者存取權限設置及變更、特殊存取權限、個人資料存取

  (3) 使用者責任

  (4) 系統及應用存取控制：資訊存取限制、保全登入程序、通行碼管理、特殊權限

資訊系統購置、發展及維護安全管理

審查要項

11. 訂有資訊系統外包管理規定及程序，且內容至少須包含以下事項：
- A. 人體生物資料庫資訊系統之建置與維護承作者，應規範及限制其可接觸之系統與資料範圍。
- B. 嚴禁核發承作者長期之系統辨識碼及通行密碼。
- C. 承作者執行建置維護作業，應在人體生物資料庫人員監督下進行。
- D. 承作者應對資訊處理設施、系統之變更進行管制。

ISO/IEC 27001:2013對應

- A.14 系統獲取、開發及維護
  - (1) 資訊系統劃分及安全要求：資訊安全規格、網路應用服務範圍、應用服務交易保護
  - (2) 開發及支援之資訊安全：系統開發資訊安全、系統變更控制程序及管理審查、開發環境、委外開發、安全測試、系統驗收
  - (3) 系統測試及測試資料保護
- A.15 供應者關係
  - (1) 供應者關係之資訊安全：供應者關係管理、安全性協議、技術資訊資料等供應鏈
  - (2) 供應者服務交付管理：供應者服務監視及審查、服務變更審查

資訊資產之管理

審查要項

12. 訂有資訊資產管理規定及程序，且內容至少須包含以下事項：
- A. 資訊設備移出設置者時，須經資訊安全主管核定，始得放行。
- B. 各項儲存設備報廢時，應核定其勘用狀況並進行必要之清除動作，始得辦理報廢。
- C. 發現有不明人士未經許可擅接網路之情事，應立即通知。
- D. 重要之資訊設備必須上鎖，且保存於合於電腦機房安全空間。
- E. 各項資訊設備須明訂管理責任及變更管理程序。

ISO/IEC 27001:2013對應

- A.8 資產管理
  - (1) 資產責任：資產清冊、資產擁有權、資產之使用、資產之歸還
  - (2) 資訊分級：分級、標示及處置
  - (3) 媒體處理：可移除式媒體的管理、媒體的汰除、實體媒體傳送

實體及環境安全管理

審查要項

13. 訂有實體及環境安全管理規定，且內容至少須包含以下事項：
- A. 僅有授權人員可以進出安全區域。
- B. 具有辦公桌面淨空政策，減少文件及儲存媒體等在正常辦公以外時間遭未經授權人員取用、遺失、篡改或破壞的機會。
- C. 定期維護設備機制，確保其持續運作並降低電力故障或異常之影響。

ISO/IEC 27001:2013對應

- A.11實體及環境安全

  (1) 安全區域：實體安全周界、實體進入控制措施、空間及設施保全、外部及環境威脅、工作區域之保全、物料交付及外部人員活動區域

  (2) 設備：設備安置及保護、電力等公用服務保障措施、佈纜安全、設備維護、財產攜出、安全區域外設備及資產的安全、設備汰除或再利用、無人看管設備管理、桌面淨空及螢幕淨空

業務持續及回復管理

審查要項

14. 訂有年度資訊安全稽核計畫，且內容至少須包含以下事項：
- A. 年度安全稽核計畫應視需要不定期進行專案稽核。
- B. 稽核紀錄應永久保存。
- C. 提供第三人使用之生物檢體及相關資料、資訊，應於契約內納入資訊安全之要求，且得對第三人進行資訊安全稽核。
- D. 稽核計畫、稽核報告結果及改善計畫，應送倫理委員會審查。
- E. 倫理委員會得視必要，指派人員會同稽核。

15. 訂有資料備份管理規定。

ISO/IEC 27001:2013對應

- A.17 營運持續管理

  (1) 資訊安全持續：規劃、實作、查證、審查及評估

  (2) 多重備援：確保資訊處理設施之可用性、資訊資料之可用性

密碼管理、電子簽章及資料加解密管理

審查要項

16. 訂有加解密管理規定及程序，且內容至少須包含以下事項：
- A. 機密性及敏感性資料分類管理政策及加密型式需求，如：實體隔離、非對稱式加解密、對稱式加解密、雜湊運算、多重加解密...等。
- B. 加密金鑰保管人員及備援措施、系統自動加解密作業及人員介入之加解密作業。
- C. 加密金鑰的產生及效期管理。
- D. 電子憑證的簽發及效期管理。

ISO/IEC 27001:2013對應

- A.10 密碼學
  (1) 密碼保護政策：使用者密碼管理、資料加密措施及範圍
  (2) 密碼金鑰管理

個人資料管理及去識別管理

ISO/IEC 27001:2013對應

- A.18 遵循性
  (1) 對法律及契約要求事項的遵循：適用法規及契約要求的識別、智慧財產權、紀錄之保護、個人可識別資訊之隱私及保護、密碼式控制措施的監管

審查要項

17. 訂有參與者個資管理規定及程序，且內容至少須包含以下事項：
- A. 參與者個人資料管理、員工個人資料管理。
- B. 個人資料鑑別及列管。
- C. 個人資料揭露軌跡追蹤管理。
- D. 個人資料保存及備援措施。

18. 訂有資料去識別管理規定及程序，且內容至少須包含以下事項：
- A. 個人資料類別定義及相應去識別措施。
- B. 資料去識別作業之個資替代型式：編碼、加密、去連結或其他無法辨識參與者身分之方式。
- C. 生物檢體、資料及資訊抽離個人資料的入庫流程。
- D. 個人資料管理作業及相關代碼置換或加解密程序。
- E. 去識別資料再連結的情境及處理流程。
- F. 管理稽核作業流程。

法律遵循及契約

審查要項

19. 訂有資訊系統建置、維運委託契約，且內容至少須包含以下事項：
- A. 明定廠商之資訊安全、管理責任、保密規定及建立定期稽核機制。
- B. 將「人體生物資料庫資訊安全規範」納入契約之一部分。
- C. 明定機密保持之範圍，契約期間及契約結束時所應負之義務。

ISO/IEC 27001:2013對應

- A.18 遵循性

  (1) 對法律及契約要求事項的遵循：適用法規及契約要求的識別、智慧財產權、紀錄之保護、個人可識別資訊之隱私及保護、密碼式控制措施的監管

倫理委員會審查—資訊安全

審查要項

1. 訂有機制由倫理委員會獨立審查，並定期檢討維護資訊安全管理系統，且內容至少須包含以下事項：
- A. 資訊安全政策。
- B. 資訊安全風險鑑別及處置方案。
- C. 資訊安全規定能否完整符合風險處置方案。
- D. 標準作業流程符合資訊安全規定。
- E. 資訊安全技術符合作業需求。
- F. 各機密等級資料保護措施及技術有效性。
- G. 使用者密碼及資料加解密金鑰的管理。

ISO/IEC 27001:2013對應

- A.18 遵循性

  (2) 資訊安全審查：資訊安全的獨立審查、安全政策及標準之遵循性、技術遵循性檢查

倫理委員會審查—資料保密

審查要項

2. 訂有機制由倫理委員會獨立審查，並定期檢討維護法規遵從性及各類合作契約，且內容至少須包含以下事項：
   - A. 參與者個人資料及隱私之保護。
   - B. 申請者智慧財產權保護及回饋資料之保密原則。
   - C. 生物資料(泛指生物檢體、資料及資訊)之限制使用、收案者優先保留及開放釋出原則。
   - D. 申請者生物資料使用限制條款、申請案範圍外使用之懲罰原則、申請案剩餘檢體之保留及銷毀原則。
   - E. 申請者與第三方合作關係之充分揭露，包括資金贊助及研究資料共享等說明。
   - F. 資料輸出之內容範圍、傳輸媒體及加密保護型式。
   - G. 國際傳輸附加規定。

ISO/IEC 27001:2013對應

- A.18 遵循性

  (1) 對法律及契約要求事項的遵循：適用法規及契約要求的識別、智慧財產權、紀錄之保護、個人可識別資訊之隱私及保護、密碼式控制措施的監管

倫理委員會審查—參與者資料保護

審查要項

3. 訂有機制由倫理委員會獨立審查，並定期檢討維護個人資料保護措施：
   - A. 參與者生物資料(含生物檢體、資料及資訊)應抽離個人資料後始得入庫，個人資料應另外隔離獨立管理。
   - B. 參與者個人資料之等級為機密以上，一律不得釋出。生物資料庫之合併與移轉有參與者同意書相關條款為依據者，不在此限。
   - C. 參與者個人資料之實體文件均有獨立隔離保護管理環境。
   - D. 保存個人資料之電腦設備及儲存媒體均設於實體網路隔離環境。
   - E. 可識別參與者身分之文件(如參與同意書、問卷)之索引碼、生物資料庫整合外部資料之原始索引碼等，機密等級均等同個人資料。
   - F. 參與者同意書內容所包含細部選項之紀錄，均應統一建檔管理以作為生物資料篩選及釋出之依據。
   - G. 訂有參與者同意書變更之程序。

ISO/IEC 27001:2013對應

- A.18 遵循性

  (1) 對法律及契約要求事項的遵循：適用法規及契約要求的識別、智慧財產權、紀錄之保護、個人可識別資訊之隱私及保護、密碼式控制措施的監管

管理面上的議題分享

- 申請者的商業利益以及合理的回饋
- 申請者是否確實只將所申請生物資料用在指定的研究上
- 申請者研究專案結束後是否有確實銷毀檢體
  - 繼續保留的誘惑很大(clinical data)
- 申請者高興申請多少就申請多少?
- 申請者真的無法重新連結識別使用者身分嗎?
- 配合prospective收案入人體生物資料庫的檢體，可以被指定申請輸出嗎?
- 一次申請，多次提領
- 去識別並不完全可靠
- 如何保障參與者的檢體只用在他所授權的範圍內?
- 收檢的醫師可以申請指定自己收檢的檢體來使用嗎? 他自己有自己的研究資料庫，參與者是自己的病人還在持續追蹤
- Cohort study收存的檢體(多次回診重複採檢的檢體)轉生物資料庫後的應用
- 一次同意，多次採檢 (如癌症病友定期追蹤，Prospective Study收案同時轉生物資料庫)
- 參與者如何被回饋受益? 告知有用在那些研究案上面，心靈的滿足

- 感染性檢體，microbiota檢體
- 未來的形式，只能申請可複製資料，管制申請原始檢體
- 只有電腦資料(包含實驗室資料)的研究資料庫，算不算人體生物資料庫?
- 全基因體序列，算不算人體生物資料庫的範圍?
- 大數據資料整合，資料標準EEC(CDA R2), CDE, FHIR，為了符合真實世界驗證的需求，建議盡早開始使用FHIR

謝謝聆聽