107年度人體生物資料庫查核作業說明會

查核基準說明及經驗分享
第四章

講師：傅昶叡　博士
服務機關：長庚紀念醫院臨床試驗中心資訊組

簡報大綱

- ✓ 查核基準及評分說明
  - ✓ 第四章 資訊安全管理
- ✓ 實務經驗分享
- ✓ Q&A

查核基準項數－第四章 資訊安全管理

查核基準	基本項目	可選項目	總項數
第四章 - 資訊安全管理	8	0	8
備註：「可」係指依審查會實際運作情形可選擇免評之條文。			

107年度查核基準及評分說明修正一覽表

項次	查核基準	修正說明
第四章 資訊安全管理		
4.3	人體生物資料庫系統應有人員權限管理機制**並嚴格管制**遠端維護	修訂查核基準及符合項目
4.6	安全區域應有門禁管制之機制並具錄影監控設備。	修訂符合項目及註解。

查核前準備

- 受查人體生物資料庫於查核前，宜進行內部資訊安全稽核作業並留有紀錄，以利委員實地查核審閱。

第四章

資訊安全管理

4.1 應有完善之資料與設備的管理機制(如：資訊系統畫面應無法辨識參與者個人資料、有定期更新系統帳號密碼機制) (1/4)

- 符合：下列項目皆符合者

1. 設有資訊系統及設備之管理機制，並落實執行且備有紀錄。
2. 電腦系統需有定期更新系統帳號密碼機制並有紀錄。
3. 電子資料應有備份機制，以防止資料滅失。
4. 正式營運之人體生物資料庫資訊系統，其帳號密碼及權限設定僅能由不涉及人體生物資料庫檢體相關業務之專責帳號管制人員維護。帳號管制人員在資訊系統上除帳號管理的權限外，亦不得有執行人體生物資料庫相關業務之權限。備援系統的管理亦同。
5. 具備定期資訊安全稽核計畫，稽核作業必須由人體生物資料庫單位以外之工作人員執行，且須留存歷史稽核紀錄備查。

4.1 應有完善之資料與設備的管理機制(如：資訊系統畫面應無法辨識參與者個人資料、有定期更新系統帳號密碼機制) (2/4)

6. 資訊系統不得顯示任何可據以辨識檢體提供者(參與者)身分之資料。資料庫檔案在參與者之辨識應由具備唯一性，且無法推斷使用者身分之代碼代替，該編碼需具備跨檔案的一致性，用以作為多檔案串聯之鍵值。

- 部分符合：上列符合項目任一項目不符合者。
- 不符合：上列符合項目任二項目不符合者。

[註]

1.除正式營運系統及指定備援系統以外，包括開發或測試的系統均僅能儲存虛構之資料，不得儲存正式參與者之資料。

4.1 應有完善之資料與設備的管理機制(如：資訊系統畫面應無法辨識參與者個人資料、有定期更新系統帳號密碼機制) (3/4)

[註]

2.文件檔案需區分機密等級，且均需存放於受管制的檔案室或安全區域內之上鎖櫥櫃。依資料機密等級區分個人保管之檔案及集中保管之檔案，集中保管之檔案須由指定專責人員管理檔案進出。文件檔案管理的稽核，應納入資訊安全稽核計畫定期執行。

評量方法及建議佐證資料：

1.資訊系統及設備管理文件。
2.訂有資訊管理及文件管理相關作業規範。
3.年度稽核計畫及歷史稽核紀錄文件。
4.資料備份機制及說明。

106年度委員共識：

符合項目第3項所提應有備份機制，係指須有備援系統或風險機制即可，無須異地備援。

4.1 應有完善之資料與設備的管理機制(如：資訊系統畫面應無法辨識參與者個人資料、有定期更新系統帳號密碼機制) (4/4)

Q & A：

Q：有關基準4.1中所提及之資訊異地備份問題，醫院目前就只有一個，且符合ISO27001標準的地點，那如果還要設另一個異地備份地是否也需符合ISO標準，規範未說明，且該設在哪裡？

A：目前尚未要求異地備份需符合ISO27001標準，惟須確保若出現問題，有其處理機制。

Q：有關基準4.1符合項目4所提，若聘任專任人員管理帳號密碼及權限設定，業務職掌上將會受到限制，另「不得有執行Biobank相關業務之權限」是指檢體業務、資訊業務或全部皆是？

A：建議本年度可由不會實際接觸到檢體業務的人，負責人體生物資料庫資訊系統帳號、密碼及權限設定。

委員常見意見：制定稽核計畫據以辦理，留有紀錄備查。

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妥適(1/2)

- 符合：下列符合項目皆符合者。
  1. 訂有生物檢體建檔編碼時去辨識化之作業程序及解密管理審查流程。
  2. 訂有可辨識資料保存管理機制。
- 不符合：上列符合項目任一項目不符合者。

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妥適(2/2)

[註]

可辨識資料及身分代碼對應資料，應由不涉及人體生物資料庫檢體相關業務之專責人員管制與保管，文件檔案保管於安全區域內之上鎖櫥櫃。

評量方法及建議佐證資料：

1.可辨識資料保存管理文件。

2.生物檢體建檔編碼去辨識化及回復之作業程序文件。

4.3 人體生物資料庫系統應有人員權限管理機制並嚴格管制遠端維護(1/2)

107年修訂

- 符合：下列項目皆符合者。
  1. 訂有人體生物資料庫系統及相關人員權限管理機制。
  2. 人體生物資料庫系統有連接網路者，僅允許由已簽保密協定之機構內資訊人員或合約廠商人員，使用設置於機構內部安全區域內的電腦終端設備，連線受管制之區域網路進行遠端系統資料庫維護作業。
  3. 資訊系統應具備防範冒用帳號之措施，例如使用者畫面必須顯示使用者的姓名及系統角色名稱。
  4. 資訊系使用者通行密碼應定期強制更新，更新周期不得超過6個月。
- 部分符合：上列符合項目任一項未符合。
- 不符合：未符合項目第1點或符合項目有二項以上未符合。

4.3 人體生物資料庫系統應有人員權限管理機制並嚴格管制遠端維護(2/2)

107年修訂

評量方法及建議佐證資料：

1.訂有人體生物資料庫人員權限管理機制。

2.現場由系統管理者操作，檢視伺服器遠端連線相關系統設定。

委員常見意見：

1.資料外洩風險，改採人員到場維護方式，在監督下進行系統維護作業。

2.應檢討人員權限管理機制是否適當。

3.電腦登錄畫面於離開時未登出。

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(1/2)

- 符合：訂有人體生物資料庫系統定期實施弱點掃描，並提供完整弱點掃描報告及相關紀錄供查核。
- 部分符合：人體生物資料庫系統未定期實施弱點掃描。
- 不符合：未訂有人體生物資料庫系統定期實施弱點掃描作業辦法。

[註]

人體生物資料庫資訊系統已通過ISO27001認證，可提供相關佐證資料。

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(2/2)

評量方法及建議佐證資料：相關弱點掃描報告紀錄。

106年度委員共識：原則上系統弱點掃描大多以委外作業，故查核時可請受查單位提供完整弱點掃描報告及相關紀錄供查核。

委員常見意見：請外部專業機構定期實施弱點掃描。

4.5 應訂有各項儲存設備報廢管理作業程序，避免內存資料外洩(1/2)

- 符合：下列項目皆符合者。
  1. 訂有儲存設備報廢管理作業程序，並有完備報廢紀錄可供查核。
  2. 儲存設備報廢應包含資料報廢及實體報廢，資料報廢須以格式化有效抹除儲存設備內所有儲存資料。實體報廢則是須以有效的破壞性方式銷毀儲存設備並確認設備不可再使用。
- 部分符合：有訂定儲存設備之報廢管理作業程序，但未確實執行。
- 不符合：未訂有儲存設備之報廢管理作業程序。

4.5 應訂有各項儲存設備報廢管理作業程序，避免內存資料外洩(2/2)

[註]

人體生物資料庫資訊系統已通過ISO27001認證，可提供相關佐證資料。

評量方法及建議佐證資料：
儲存設備報廢管理作業程序及記錄。

委員常見意見：應落實報廢資訊儲存設備之實體破壞，並確保設備無法再使用。

4.6 安全區域應有門禁管制之機制並具錄影監控設備(1/2)

107年修訂

- 符合：下列項目皆符合者。
  1. 安全區域訂有門禁管制機制，且須可調閱至少6個月人員進出紀錄。
  2. 安全區域設有錄影監控系統，須具備足夠的影像解析度，及可調閱至少兩個月前影像。
- 部分符合：未有門禁管制機制或未設置錄影監控設備等相關佐證文件
- 不符合：安全區域未訂有門禁管制機制或未設置錄影監控設備。

4.6 安全區域應有門禁管制之機制並具錄影監控設備(2/2)

107年修訂

[註]

1.人體生物資料庫資訊系統已通過ISO27001認證，可提供相關佐證資料。

2.安全區域係指具有嚴密實體區隔與安全管制措施，可確實阻止未經授權者進入的區域。

評量方法及建議佐證資料：

門禁安全管理規範及紀錄。

委員常見意見：門禁系統應有回溯性紀錄。

4.7 訂有安置或保護設備（重要之資訊設備是否上鎖）相關機制，以降低環境之威脅、災害及未授權存取產生的風險

- 符合：下列項目皆符合者。

  1. 訂有設備安置之標準作業程序。
  2. 訂有重要資訊保護作業規範。

- 不符合：上列任一項不符合者。

[註]

人體生物資料庫資訊系統已通過ISO27001認證，可提供相關佐證資料。

評量方法及建議佐證資料：
訂有重要資訊保護作業規範。

4.8 訂有定期維護設備機制，以確保其持續運作並降低電力故障或異常

- **符合**：訂有定期維護設備機制之作業規範或程序，且資料完備可查。
- **部分符合**：有訂定設備機制之作業規範或程序，但未確實執行。
- **不符合**：未訂有定期維護設備機制之作業規範或程序。

[註]

人體生物資料庫資訊系統已通過ISO27001認證，可提供相關佐證資料。

評量方法及建議佐證資料：

設備維護相關文件。

實務經驗分享

- 針對資訊設備管理、資料保存等分享經驗談
- 針對人體生物資料庫個資管制說明

生物資料庫實體安全

- 包括**個資管制室、資訊機房、檢體貯存庫、檔案室、實驗區、辦公區等**，均為各自獨立區隔且有門禁管制的實體空間

- 通用需求
  - 中央連線門禁管制及進出紀錄
    - 設定人員各區域進出權限及可進出時段，以及員工離職後終止進出權限
    - 保留人員進出紀錄，確保不可竄改
  - 監視攝影機
    - 須確保監視攝影機能免受惡意破壞
    - 各安全區域門禁監視器須裝於門內安全區域，朝出入口方向攝錄人員進出影像
    - 非安全區域之監視器以兩兩相互監視方式防止人為破壞

實體區隔門禁管制之安全區域

- 個資管制室
  - 人體生物資料庫個資管制作業必須在獨立的個資管制室內，使用管制室之資訊設備進行。
  - 個資管制室僅允許人體生物資料庫之指定個資管制員進入，其他人員因設備維護、稽核等須進入者，須登記進出紀錄簿後在個資管制員全程陪同下進入。
  - 為網路封閉環境，僅允許管制室內資訊周邊設備相互連線，不可與管制室以外其他網路或設備進行連線。
  - 與外部資訊系統資料交換需求者以離線媒體進行。
  - 含個資資料檔案備份時均必須加密並以密碼保護後，始得攜出個資管制室至其他安全區域貯放。

實體區隔門禁管制之安全區域

- 資訊機房
  - 用於管理人體生物資料庫管理系統之伺服主機，機房管理含主機備援及資料備份管理均應符合ISO27001要求。
  - 可由人體生物資料庫自行獨立設置機房管理，或委由機構內其他經ISO27001認證之電腦機房代為管理。
  - 實體主機連線之網路必須為獨立區域網路，僅允許人體生物資料庫範圍內之人員設備連線，以及指定之系統管理人員設備連線使用。委託其他電腦機房代管者，可設定虛擬區域網路(VLAN)並透過ACL達到該管制目的。
  - 人體生物資料庫管理系統伺服主機之系統維護，僅允許由指定之機構內資訊人員或合約廠商，使用人體生物資料庫的電腦終端設備，連線受管制之區域網路進行遠端系統維護作業。

生物資料庫資訊管理系統 (以功能區分)

- 個資管理系統
  - 管理包含個資的參與者資料及檢體提供者知情同意書
  - **不存放生物資料庫檢體資訊，可存放外部匯入資料**
  - 去識別化資料與識別資料連結對應
  - 提供**去識別**、**去連結**、**再識別**、**資料更新**功能
  - 連接**個資管制室內部封閉網路(不得連接其他網路)**，使用者為**個資管制員**

- 生物資料庫管理系統
  - 生物檢體物流、內部作業管理、申請案管理審查
  - **完全去識別化，禁止存放任何個資或可用以追溯個資的對應資料**
  - 連接**受防火牆保護之生物資料庫專用獨立區域網路**，使用者為**生物資料庫人員**
  - 在管制IP位址原則下，提供雲端查詢服務給生物資料庫查詢檢索系統或外部審查資訊系統
  - **必須有效防杜網路攻擊，定期弱點掃描**

- 生物資料庫查詢檢索系統 (optional)
  - 供研究人員查詢符合指定篩選條件的檢體存量
  - 獨立於生物資料庫管理系統之外，**不可連接任何資料庫系統**
  - 連接**機構內部區域網路或公眾網路**，使用者為**已註冊且經身分驗證的外部使用者**
  - **必須有效防杜網路攻擊，定期弱點掃描**

個人資料的範圍

- 可直接辨識身分資訊(具備全域唯一性)
  - 姓名、身分證統一編號、護照號碼
  - 指紋、視網膜、靜脈分布
- 可間接辨識身分資訊
  - 聯絡方式、社群軟體ID
  - 機構資料庫索引碼
    - 醫院病歷號、門診單號、藥囑單號、收據單號、賣場客戶編號、訂單編號等
- 可組合推敲身分資訊
  - **基因、醫療、健康檢查**
  - 性別、生日、居住區域、特徵
- 身分已知下的敏感資訊
  - **醫療、性生活、健康檢查、犯罪前科**
  - 婚姻、家庭、教育、職業、病歷、財務情況、社會活動

個資管理相關操作

- 去識別 (de-identification)
  - 管制對象：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 (delink)
  - 管制對象：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)

- 再識別 (re-identification)
  - 管制對象：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：在個資管制室協助下調閱對應資料，稽核人員只能問與看，不能操作資訊系統

- 資料更新，追加欄位
  - 管制對象：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：個資管制室依原申請案範疇及替代索引欄位編碼，產出最新版資料檔提供給申請者。

個資管理相關操作--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
  - …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**

個資管理相關操作--去識別

- 知情同意書
  - 標的欄位：檢體提供者身分代碼、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 → 採用替代索引值識別
    - 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

個資管理相關操作--去連結

- 目的
  - 申請者無法透過其他途徑重新連結生物資料提供者身分
  - 申請資料難以用於申請範圍以外用途
  - 不同申請案資料的彙整難度高，避免申請者累積私庫用於其他用途

- 處理方式
  - 同去識別處理模式，但所有替代索引代碼唯一性縮小至申請案範疇。
    - **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)。

個資管理相關操作--再識別

- 目的
  - 因稽核現場抽查，需由檢體反查調閱同意書時
  - 因異常事件追查所需

- 處理方式
  - 由個資管制室對所查詢檢體或個案，調閱檔案追查來源參與者身分
  - 依照檢體提供者身分，因應查核需要調閱相關佐證文件
  - 因異常事件追查，須將檢體或參與者再識別結果輸出者，應以編號列管之正式文件交付予申請者並保存簽收紀錄。

生物資料庫管理系統

- 檢體物流管理
- 檢體處理分裝
- 檢體入出庫管制
- 檢體品質管理
- 檢體庫存狀態追蹤
- 資料檢索篩選
- 生物資料申請案管理
- 生物資料研究數據回饋
- 稽核軌跡功能

- 應符合GLP、ISO 17025精神
- 應盡可能符合21 CFR part 11

檢體收案、運送、入庫與去識別參考作法

- 檢體收案（檢體收集單位）
  - 參與者填寫知情同意書(每一文件事先配予參與者編號)
  - 採集檢體並以參與者為單位裝盒或袋，外部標貼參與者編號
  - 檢體處理分裝至已貼檢體編號之容器並登錄於運送清單(參與者編號，檢體編號)
  - 冷凍暫存，隔日以含保冷材與溫度記錄器之包裹寄出(冷凍檢體、運送清單、同意書)

- 包裹接收，檢體入庫
  - 包裹收件後，依運送清單清點檢體狀況後入庫(登錄參與者編號與檢體系統編號)，運送清單連同參與者同意書送至個資管制室
  - 產生新的知情同意書系統編號，標貼於原紙本文件並掃描存檔。
  - 個資管制室依知情同意書內容進行參與者資料建檔，產生新的參與者系統編號
  - 依照運送清單內容將已登錄入庫的檢體與參與者建立連結
  - 知情同意書與運送清單紙本文件歸檔

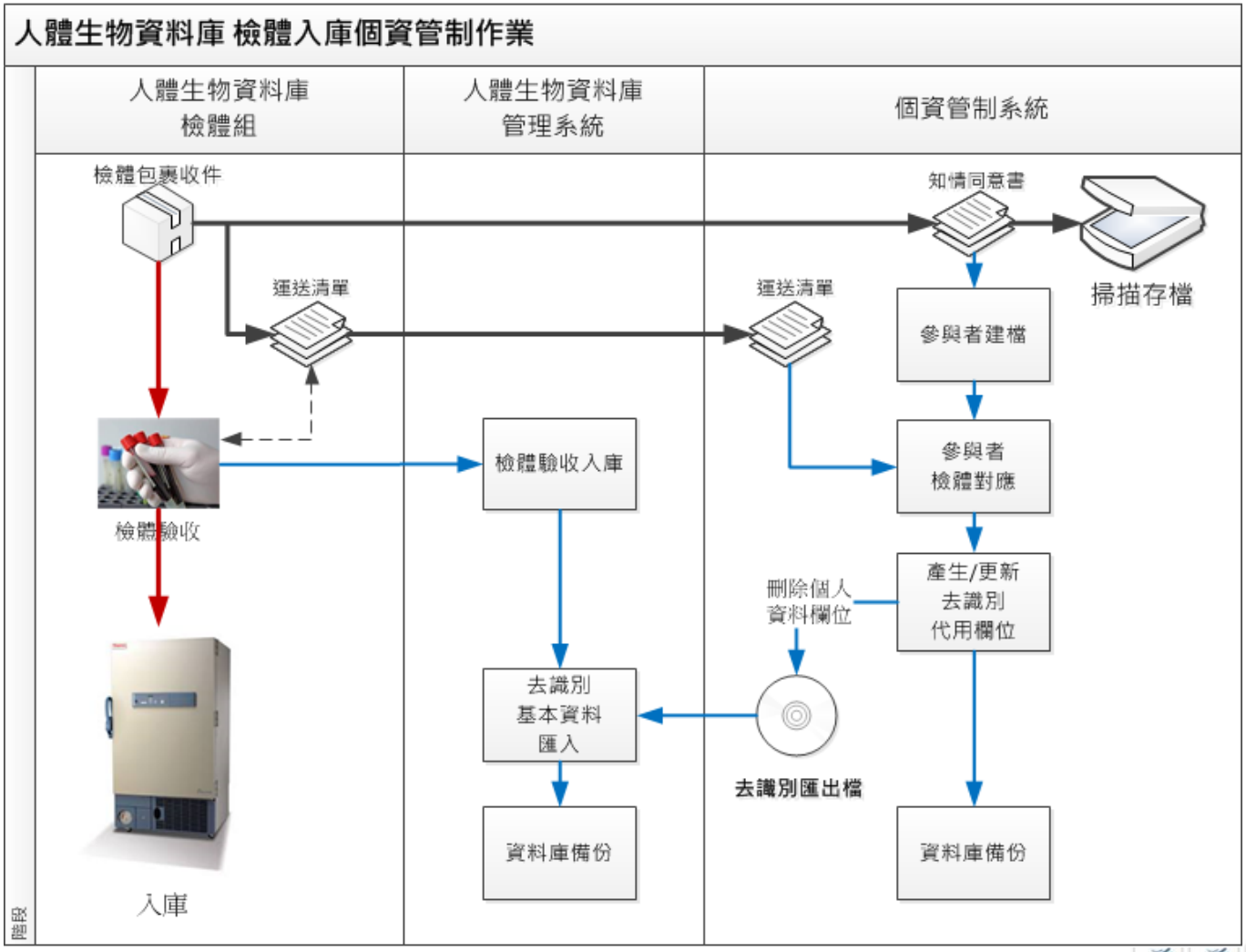
檢體入庫相關個資管制技巧

- 人體生物資料庫管理系統跟個資管制系統各自獨立，均需維護參與者資料，但在人體生物資料庫管理系統中該參與者資料是去識別的。

- 人體生物資料庫管理系統內部編碼管制
  - 參與者編號在印製空白知情同意書時配號，而非實際收案時
  - 一個容器一個檢體編號，檢體編號在備置容器時配號，而非實際收檢時
  - 任何檢體作業均只能以檢體編號識別檢體，**不能以參與者編號識別檢體**
  - 所有編碼應以使用簡單的流水號為原則，編碼原則可夾帶內部管理用的分類資訊(如檢體類別、貯放溫度別)，但**不能夾帶其他實體對應或外部對應識別資訊**(例如參與者編號、病歷號碼、醫囑單號、檢驗單號、冰箱編號、貯存盒編號等)

- 個資管制系統內部編碼原則與個資建檔
  - 參與者是在實際收案且檢體寄達生物資料庫後，才會新建參與者個人資料
  - 使用與人體生物資料庫管理系統相同的參與者編號系統。

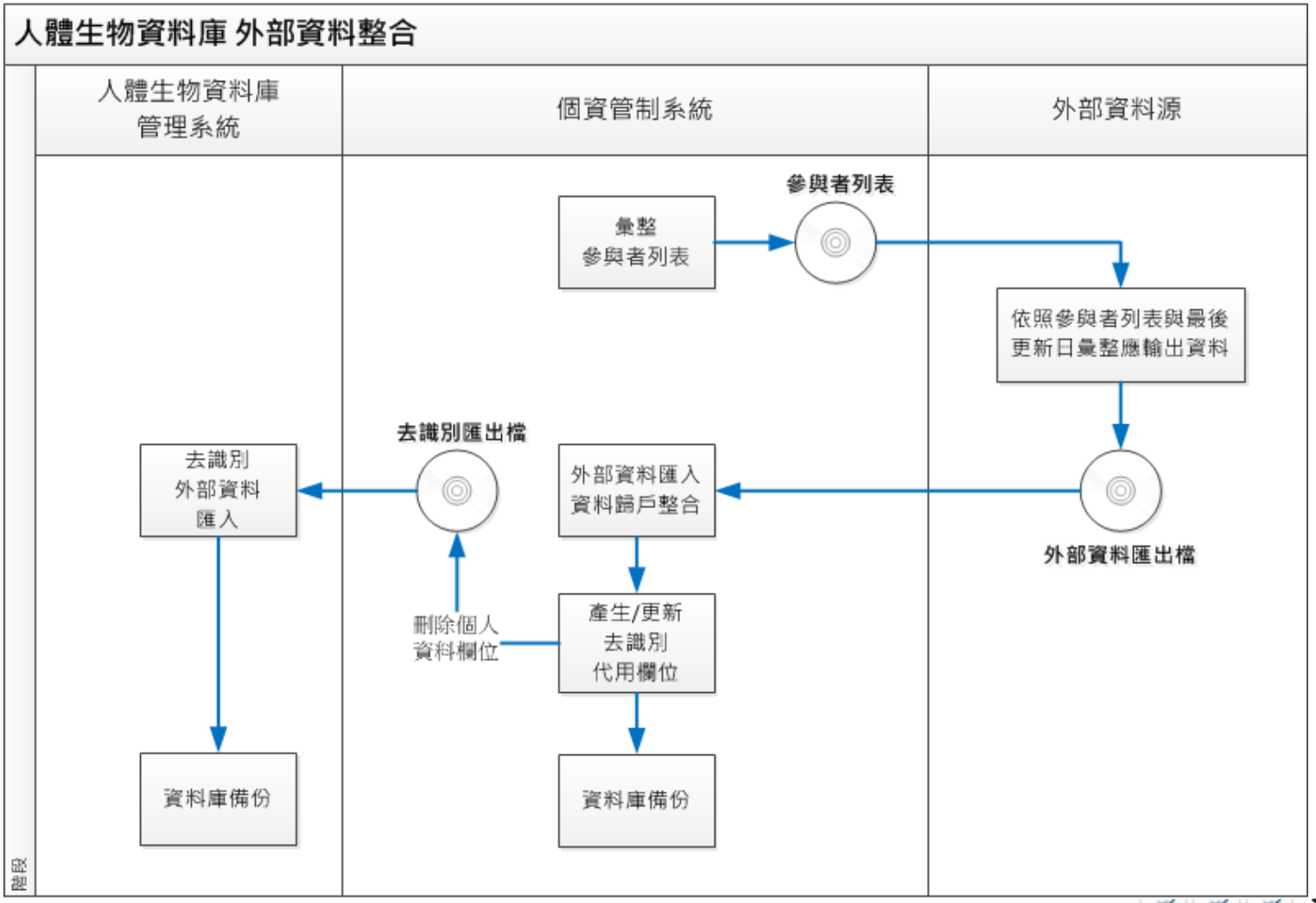
個資管制作業：檢體入庫與去識別



整合外部資料庫/外部資料定期更新

- 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取得參與者關聯的**完整資料**(係指合作範疇內)
- 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

整合外部資料庫



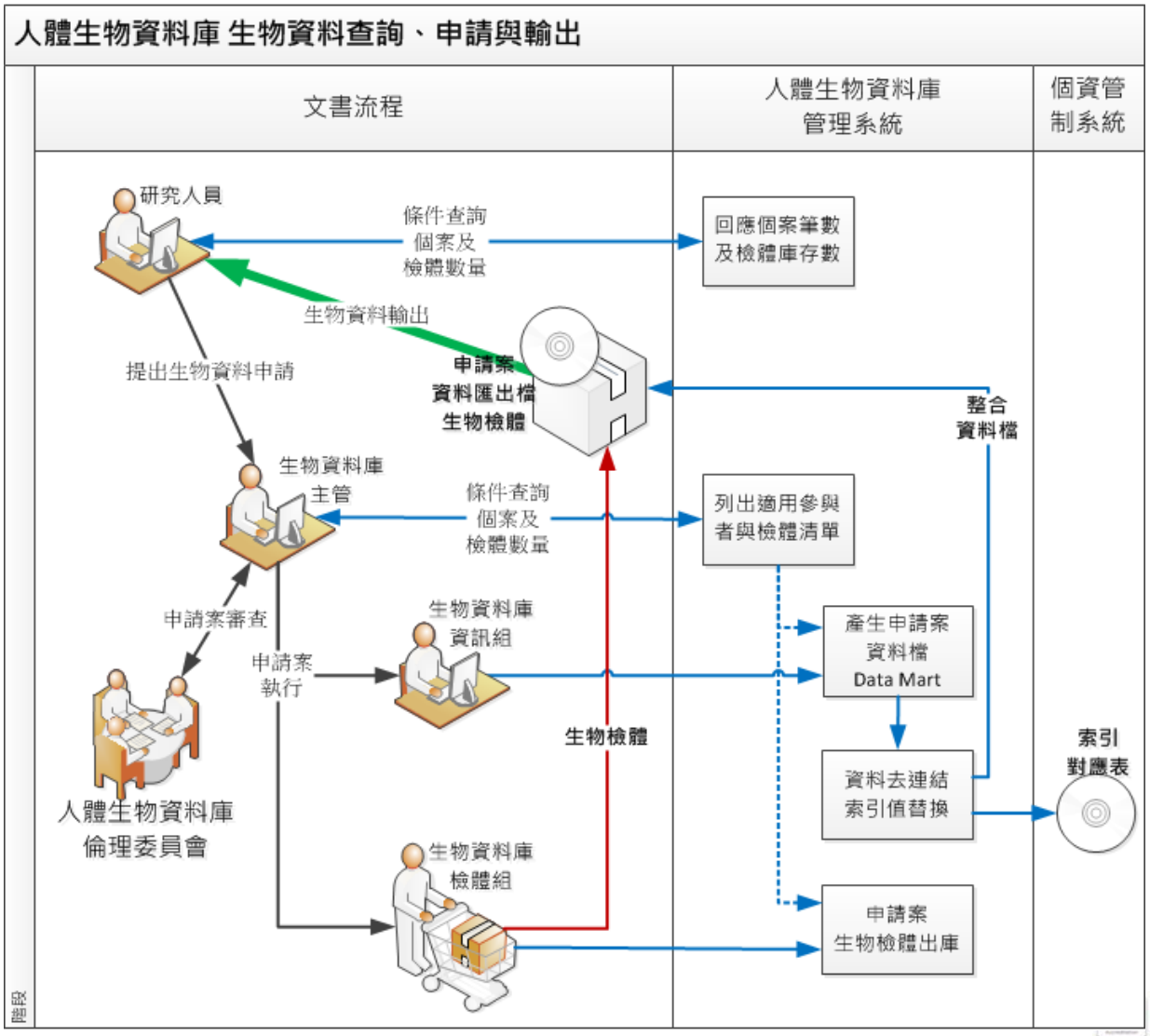
生物資料查詢、申請與輸出

- 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

- 準備申請範圍之資料
  - 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。

- 檢體提領出庫
  - 確保檢體提取的正確性
  - 確認檢體狀態，如有異常必須回報應變
  - 檢視檢體過往處理貯存歷程
  - 可靠的保溫措施，確保檢體輸出品質

生物資料查詢、申請與輸出



舊案資料更新或欄位追加

- 目的
  - 使用者申請舊案資料更新或追加資料欄位

- 處理方式
  - 由個資管制室調出舊案所有替代索引代碼與原識別代碼的對應表
  - 重新整理資料檔，進行去連結後交付予申請者

其他選擇性功能

- 生物資料庫查詢檢索系統
  - 依照各類資料欄位篩選條件，查詢檢體庫存量

- 檢體研究資料回饋機制
  - 外部資料交換
    - 協作生物實驗室資料交換
    - 樣板資料交換格式
  - 研究者自行輸入回饋
    - 需要資料收集平台
    - 制式化表單

Q&A

謝謝聆聽

說明會提問將納入本年度委員共識確認，
後續將放置本會網站供各界下載