110年度人體生物資料庫查核作業說明會

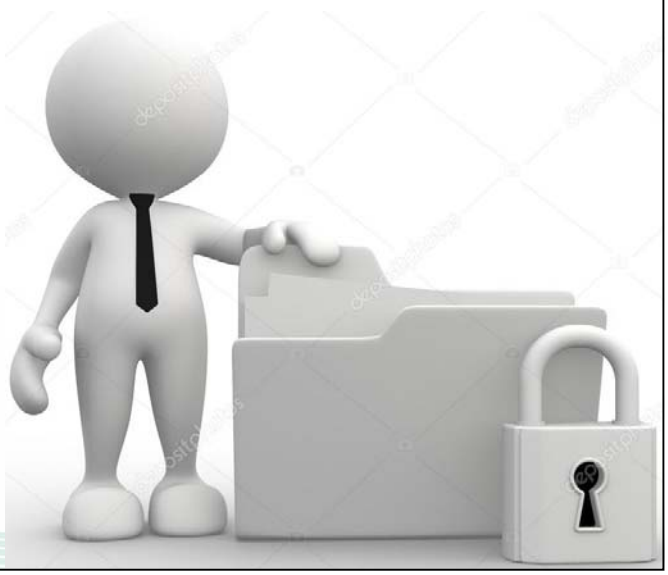
查核基準及評分說明-第四章

秀傳醫療體系

劉　立 醫療資訊副院長

大綱

- 查核基準及評分說明
  - 第四章 資訊安全管理



查核基準項數

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。			

110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		
4.1	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）	新增評分說明、修訂及新增評量方法及建議佐證資料
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	修訂評量方法及建議佐證資料
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	修訂評量方法及建議佐證資料

110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		
4.5	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	修訂評量方法及建議佐證資料
4.6	實體隔離區應有門禁管制之機制並具錄影監控設備	修訂查核基準名稱、評分說明與評量方法及建議佐證資料
4.7	訂有安置或保護設備相關機制，以降低環境之威脅、災害及未授權存取產生的風險	修訂查核基準名稱與評量方法及建議佐證資料
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	修訂評量方法及建議佐證資料

查核基準及評分說明

第四章

資　訊　安　全　管　理

第四章 資訊安全管理

《重點說明》

為防止個人資料遺失、誤用，人體生物資料庫應有完善的資訊管理及安全相關政策與作業規範，確保資訊具有「保密性」、「安全性」與「完整性」等必備條件，本章節之查證重點包含：

✓ ***完善的資訊管理及安全相關政策與作業規範***

✓ ***確保資訊具有「保密性」、「安全性」與「完整性」等必備條件***

✓ ***明確訂定資訊保密相關措施***

✓ ***門禁管理機制***

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）(1/5)

110年修訂

●**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應由不實際接觸檢體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。

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）(2/5)

110年修訂

●**符合**：下列項目皆符合者。

5. 經電子郵件或其他電子方式對外傳送之資訊，應以倫理委員會認可之技術加以處理；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。
6. 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。
7. 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。

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）(3/5)

110年修訂

●**部分符合**：符合項目任一項未符合者。

●**不符合**：符合項目任二項未符合者。

[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。

2.儲存去識別資料之電腦主機，可連結機構內部網路或可放置於機構的資訊機房。

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）(4/5)

110年修訂

評量方法及建議佐證資料：

1.資訊系統及設備管理文件。

2.資訊系統與設備管理作業程序。

3.人體生物資料庫資訊管理作業程序（含人員權限、備份、弱點掃描、資訊安全稽核計畫、重要資訊保護）。

4.年度稽核計畫及歷史稽核紀錄文件。

5.資料備份機制及說明。

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）(5/5)

110年修訂

109年度委員共識

1.符合項目第3項所提應有備份機制，係指係指人體生物資料庫有定期異地（有一定距離且非同棟）備份即可，無須異地備援。

2.符合項目第4點之帳號密碼修改應留有紀錄，且應有不得竄改之機制。

106-109年度查核常見意見

1.文件檔案區應區分機密等級，並標示於文件或儲藏櫃上 。

2.保存參與者個資之電腦應設有密碼保護且帳號權限應由專責人員維護。

3.電子資料應有定期異地備份機制，以防止資料減失。

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(1/3)

110年修訂

●**符合**：下列項目皆符合者。

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。
3. 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。

●**不符合**：符合項目任一項目未符合者。

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規範(2/3)

110年修訂

[註]

1. 去辨識資料的解碼作業流程，為將資料恢復為可辨識身分的申請作業流程。該流程必須具備完善的管理審查機制，以確保參與者身份資料的正當使用。
2. 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. 加密、解密作業程序。
3. 可辨識個人資料文件管理作業程序。

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(3/3)

109年度委員共識

1.符合項目第3點資料庫檔案不須限定以代碼代替，實地查核時確認該機制可作為多檔案串聯之鍵值即符合。

2.資料解密作業為確保資訊安全，不應僅有1人擁有金鑰解密權限即可回復資料，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。

106-109年度查核常見意見

參與者同意書與生物檢體應有不同之編碼，且應避免生物檢體人員處理參與者同意書。

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(1/3)

110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.資訊系統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。

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(2/3)

110年修訂

- **部分符合：**符合項目任一項未符合。
- **不符合：**未符合符合項目第1點或符合項目有二項以上未符合。

評量方法及建議佐證資料：

1. 人體生物資料庫資訊管理作業程序（含人員權限、備份、弱點掃描、資訊安全稽核計畫、重要資訊保護）。
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。

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(3/3)

109年度委員共識

1.符合項目第2點「內部安全區域內」所指為實體區域，非虛擬空間。

2.符合項目第3點係指使用者畫面必須顯示使用者姓名，本年度不強制顯示系統角色名稱。

106-109年度查核常見意見

宜發展人體生物資料庫資訊系統，較能完善權限管理機制。

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：

1.相關弱點掃描報告紀錄。

2.已實體隔離網路之資訊系統，得免實施網路弱點掃描。

109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。

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)

110年修訂

●**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)

110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。

評量方法及建議佐證資料：

資訊儲存設備報廢管理作業程序。

4.6實體隔離區應有門禁管制之機制並具錄影監控設備(1/2)

110年修訂

●**符合：**下列項目皆符合者。

1.實體隔離區訂有門禁管制機制，且須可調閱至少6個月人員進出紀錄。

2.實體隔離區內、外設有錄影監控系統，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：**實體隔離區未訂有門禁管制機制或未設置錄影監控設備。

4.6實體隔離區應有門禁管制之機制並具錄影監控設備(2/2)

110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。

評量方法及建議佐證資料：

設施設備維護與門禁安全管理作業程序。

106-109年度查核常見意見

1.錄影監控裝置應確實達到門禁監視。

4.7訂有安置或保護設備相關機制，以降低環境之威脅、災害及未授權存取產生的風險

110年修訂

●**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：**任一項未符合者。

[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：

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

110年修訂

●**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。

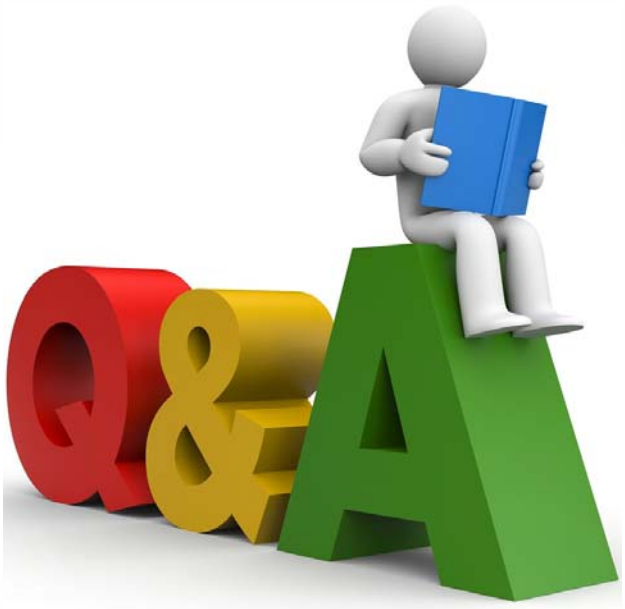
[註]

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：

1.設備維護相關文件

2.資訊系統與設備管理作業程序



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