高雄榮民總醫院人體生物資料庫資訊安全規定

民國101年3月31日 倫理委員會通過
民國103年10月17日 修訂
民國110年8月27日EGC renew
民國 113 年 3 月 29 日 EGC 修訂
衛部醫字第1130120024號函核定

壹、 目的

為保障人體生物資料庫參與者權益，並確保人體生物資料庫資訊相關作業符合機密性、完整性及可用性之要求，特制定本規定。

貳、 依據

「人體生物資料庫管理條例」、「人體生物資料庫資訊安全規範」及「人體生物資料庫查核基準」。

參、 適用範圍

本規定適用於本院已向主管機關申請，依法設置之人體生物資料庫之相關營運作業。

肆、 資訊管理單位組織、權責及分工

人體生物資料庫設有資訊管理任務編組，其權責依分工說明如下：

一、 資訊主管:督導、維護生物資料庫資料、資訊之安全管理，及其他與生物資料庫之資訊安全有關事項。

二、 資訊管理人員：負責生物資料庫資訊、資料管理，及資料篩選、整理與輸出作業。資訊管理人員由不涉及人體生物資料庫檢體相關業務之人員擔任,且除與生物資料庫推展及營運相關之研究計畫外，與研究人員不得互為兼任。

三、 系統管理人員：負責資訊系統之開發維護管理。系統管理人員不得兼任資訊管理人員，亦不得接觸檢體業務。

伍、 人員管理及資訊安全訓練

一、 人體生物資料庫人員均簽署「人體生物資料庫保密及利益迴避同意書」，對於業務上所知悉、持有之相關資料應保守機密，不擅自揭露或洩漏。

二、 人體生物資料庫人員之資訊系統權限依本院「人體生物資料庫門禁管制與資訊系統授權管理程序書」規定申請開通，人員離(退)職時，應即取消使用權限。

三、 人體生物資料庫相關人員應依本院規定,每年接受資訊安全教育訓練至少3小時。

陸、 電腦系統安全管理

一、 人體生物資料庫資訊系統主機應依相關規範完成風險評鑑及管理評估作業。

二、 人體生物資料庫系統主機應安裝於設有安全保護之機房內，進出人員應有安全管控措施。

三、 機房應設置環境監控系統，值班人員可掌握機房溫、溼度

狀況，並設置消防系統，定期進行消防演練。

四、 人體生物資料庫系統主機應安裝於院內區域網路，並設置網路防火牆、防毒牆、入侵偵測設備等，與院外網路隔絕，以降低入侵風險。

五、 機房應設置不斷電系統，以確保供電穩定無虞。

六、 人體生物資料庫系統主機應安裝防毒軟體並即時更新病毒碼，定期進行系統病毒掃描作業。

七、 人體生物資料庫系統主機應定期進行系統弱點檢測及執行各項系統漏洞修補程式。

八、 人體生物資料庫系統主機資料應定期備份，以降低資料毀損風險。

柒、 網路安全管理

一、 人體生物資料庫網路系統運作之相關事宜，須遵照本院「網路安全管理程序」、「網站管理規定」、「個人電腦使用管理規定」、「電子郵件信箱管理規定」、「防火牆管理規定」辦理。

二、 人體生物資料庫有關資訊，非經本院生物資料庫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。經人體生物資料庫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。

三、 收案後所建置之人體生物資料庫之個人資料，應以實體隔離之方式建構及使用，其資訊系統採加密系統及授權金鑰管理，不得與網際網路連接。

四、 建置之人體生物資料庫資訊系統不得提供診斷埠存取控制、網路連線控制及網路路由控制。

捌、 資訊系統存取控制管理

一、 人體生物資料庫之系統存取政策及授權規定，依照本院資訊室「資訊系統存取控制管理程序」規定辦理。

二、 人體生物資料庫須有帳號權限管理制度，建立使用名冊，加強使用者通行密碼管理，並要求使用者之密碼長度及複雜度；使用者通行密碼之更新周期，依本院資訊安全管理需求決定，最長以三個月為限。

三、 具有系統存取特別權限之人員，應建立使用人員名冊，加強安全控管，並縮短通行密碼更新周期，其系統存取權限，以執行其職務所必要者為限；對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，應經審慎之授權，並定期查核其權限及活動日誌，前項最高權限人員，至少應有二人。

四、 參與者之個人資料有存取、異動、查閱時，應申請並經主管簽核後始得執行，並存檔備查。

五、 人體生物資料庫系統資料應定期每月執行備份作業，以防

止資料滅失或毀損。

六、 若因參與者變更同意範圍或退出，致應銷毀其資料時，應以不可回復之方式為之。

玖、 資訊系統購置、發展及維護安全管理

一、 人體生物資料庫系統發展及維護須依照本院資訊室「系統發展及維護之安全管理程序」之規定辦理

二、 人體生物資料庫資訊系統購置或維護若委託其他廠商辦理，委外廠商除依照前項規定辦理外，另須遵守下列規定：

（一）依照本院「資訊業務委外服務駐點人員暨維護人員管理規定」，並於委託契約中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；並將本規範納入成為契約之一部分。委託契約應明定機密保持之範圍、契約期間及契約終了時所應負之義務。

（二）對人體生物資料庫資訊系統之建置與維護之承作者，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期之系統辨識碼及通行密碼；承作者執行建置維護作業，應在本院所屬人員監督下為之。

壹拾、 資訊資產之管理

人體生物資料庫之資產的項目、擁有者及安全等級分類等，須遵守本院「資訊資產管理作業程序」規定辦理。

壹拾壹、 實體及環境安全管理

一、 人體生物資料庫進出管制依「人體生物資料庫門禁管制與資訊系統授權管理程序書」規定辦理。

二、 人體生物資料庫實體隔離機設置空間應設置消防與監控設備，人員應定期受消防教育訓練每年兩次及演練每年一次。

三、 電腦設備不使用時，應登出關機或設定螢幕鎖定保護，文件或資料如含有個人資料應有專人管理及保管。

壹拾貳、 資訊安全事件發生之通報及保全處理程序

一、 資訊安全事件發生時，應通報資訊主管，其處理程序依照本院資訊室「資通安全事件危機通報與事件管理規定」及「人體生物資料庫緊急應變處理管理程序書」辦理。

二、 資訊安全事件經查明如有致參與者權益遭受侵害，應通報主管機關並以適當方式通知相關參與者。

壹拾參、 業務持續及回復管理

一、 各項天然災害、人為或其他異常事件，可能致生物資料庫業務中斷之評估、應變、復原與檢討改善，依「人體生物資料庫緊急應變處理管理程序書」辦理。

二、 人體生物資料庫之備份作業，應依「人體生物資料庫資料儲存備份管理程序書」及「人體生物資料庫異地備份作業

程序」辦理。

三、 備份資料按月儲存,備份媒體應至少存放一份於異地儲存，且異地備份頻率每兩個月一次。

四、 每年應進行至少一次備份媒體回復測試作業。作業程序如下：

1. 倒回最近一次系統備份資料。
2. 倒回最近一次備份資料。
3. 實施資料完整性檢查。
4. 測試系統是否可正常作業。

五、 回復測試作業執行人員應於回復完成後填寫回復測試紀錄，註明回復測試結果。

六、 備份作業規劃及回復測試結果每年應進行檢討修正。

壹拾肆、 其他

一、 本規定之規劃、執行、審議由本院資通安全管理小組督導下辦理,並由資通安全稽核小組執行年度人體生物資料庫資訊安全稽核。

二、 本規定應逐年檢討並為必要之修正,經本院人體生物資料庫倫理委員會審查通過後報主管機關核定。