臺中榮民總醫院人體生物資料庫
資訊安全規定

民國 100 年 11 月 28 日 訂定，
民國 101 年 01 月 16 日 修訂，
民國 101 年 09 月 25 日 增訂，
民國 102 年 11 月 07 日 修訂，
人體生物資料庫倫理委員會審查通過。

壹、目的

一、 爲推動臺中榮民總醫院 (以下簡稱本院) 人體生物資料庫作業，符合相關法規，使本院人體生物資料庫作業有所遵循，特訂定本規定，以確保人體生物資料庫資料符合機密性、完整性及可用性之要求。

貳、依據

二、 「人體生物資料庫管理條例」、「人體生物資料庫資訊安全規範」、「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」及本院資訊安全相關規定。

參、適用範圍

三、 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

四、 人體生物資料庫設有資訊管理小組，其權責依分工說明如下：

(一) 資訊主管：由資訊室主任擔任，資訊室業管資訊安全業務組長協助，負責資訊安全管理事項之協調及推動。

(二) 資料 (及資訊) 管理人員：由人體生物資料庫管理單位選派適當人員兼任，負責資料與資訊之管理。

(三) 資訊系統維運人員：由資訊室選派系統管理人員兼任，負責系統軟硬體建置、系統運作平台之建置及維運。

(四) 以上各類人員不得互為兼任。

五、 本院設有「資通安全會報」，召集人由本院行政副院長兼任，委員由醫療及行政一級單位主管組成。負責本院資訊安全管理事項之協調及推動，並辦理資訊安全政策、規劃、執行等審議、督導事項。

六、 人體生物資料庫資料 (及資訊) 管理人員與研究人員不得互為兼任。

伍、人員管理及資訊安全訓練

七、 人員管理：

(一) 參與人體生物資料庫相關人員應依據公務人員任用法（含施行細則）、派用條例（含施行細則）、醫事人員人事條例（含施行細則）、聘用條例（含施行細則、聘用注意事項）、約僱人員僱用辦法、勞動基準法（含施行細則）、台中榮民總醫院運用醫療作業基金進用醫務人員作業要點、替代役實施條例、特約顧問管理辦法、外包管理規定、工友管理要點等相關法規及本院相關作業規定進用管理。

(二) 人體生物資料庫資訊主管、資料 (及資訊) 管理人員、資訊系統維運人員等相關人員，均應填具保密切結書。

八、 資訊安全教育訓練：

人體生物資料庫資訊主管、資料 (及資訊) 管理人員、資訊系統維運人員等相關人員每年應接受至少 3 小時 (含) 以上資訊安全相關教育訓練課程時數。

九、 參與人體生物資料庫相關人員離（退）職時，應立即取消人體生物資料庫之所有權限。

陸、電腦系統安全管理

十、 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。

十一、 人體生物資料庫系統主機應定期進行系統弱點檢測，並執行各項系統漏洞修補作業。

十二、 人體生物資料庫系統所屬設備、資訊、或軟體，未經資訊室主管或人體生物資料庫管理單位主管授權，禁止移動。

十三、 人體生物資料庫系統資料應定期進行備份，以防止資料滅失。

柒、網路安全管理

十四、 人體生物資料庫有關資訊，非經本院人體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。

十五、 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，其資訊系統不得與網際網路連接。

十六、 人體生物資料庫除個人資料以外之資料，若因業務需要需與院外單位進行資料交換時，應簽訂合作協議書，規範單位間交換資訊安全之保護措施。

十七、 人體生物資料庫各類資訊對外公告前應提交人體生物資料庫倫理委員會審查通過，並簽呈院部長官核示後公告，以避免未授權之篡改。

十八、 人體生物資料庫禁止開放遠端維護。

十九、 本院電腦網路分隔為：內部網段 (INTRANET)、隔離區 (DMZ)、及外部網段(INTERNET)，各網路區段間應以防火牆區隔，本院以外之任何外界均不得直接存取本院內部網段。

二十、 使用網路診斷埠之前應填具本院「Firewall 防火牆申請單」，註明申請時間及使用網路診斷埠範圍，經資訊室主任核准後，依申請時間及使用網路診斷埠範圍進行作業。

二十一、 由隔離區 (DMZ) 對內部網段之存取，應以單點對單點方式連結，並在特定通訊協定方式下進行存取連線。

二十二、 外部網段或任何外界對本院隔離區 (DMZ) 之連結，需明確限定允許之通訊協定。

捌、資訊系統存取控制管理

二十三、 人體生物資料庫應訂定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。

二十四、 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。

二十五、 人體生物資料庫須建立使用者註冊管理制度，設定帳號密碼登入管制措施，以避免未經授權人員存取。實體隔離室資料庫進行資料存取時，應有兩人在場。

二十六、 人體生物資料庫密碼設定應避免以下情形：長度太短 (未超過六個字元)、全部為字母或全部為數字、與個人有關資料 (如身份證字號、生日等) 等，以確保密碼安全性。

二十七、 人體生物資料庫使用者帳號密碼不得授與他人使用，並應定期更換(至少六個月更換一次)。

二十八、 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。

二十九、 人體生物資料庫系統各類人員存取、增刪、查閱、複製人體生物資料庫紀錄時，資訊系統應將執行人員、時間等資料加以記錄，存取紀錄應保存至少六個月，以備稽核與查驗需要。

三十、 人員存取記錄應定期執行備份作業，以防止資料滅失或毀損。

三十一、 人員存取紀錄調閱前應提交人體生物資料庫倫理委員會審查通過後，由資訊主管進行調閱。

三十二、 人體生物資料庫各項資料、資訊之安全措施，應依參與者之同意範

圍，進行不同等級之保護，並依同意書之變更，更改至適當等級。若因同意書之變更致應銷毀其資料時，應以不可回復之方式銷毀。

三十三、　人體生物資料庫使用者存取權限應依本院「資訊系統存取控制管理規範」進行管制。資訊主管應定期審查使用者存取權限，每六個月至少需評估一次，以防止未經正式授權程序取得特別權限。

三十四、　行動電腦設施應依本院「攜帶個人資訊設備至院內使用管理規定」進行管制。使用前應填寫「無線網路連線申請單」，登錄網路卡識別碼後，並安裝防毒軟體後才可使用。

三十五、　因任務需要需自院外連線使用本院資訊系統者，應填具本院「VPN帳號申請單」，註明申請時間及申請連線範圍，經資訊室主任核准後，依申請時間及申請連線範圍進行遠端連線作業。

三十六、　個人資料相關作業應避免以網路方式傳送。若因業務需要必須以網路傳送時，應使用以下技術進行控制：以專線網路點對點進行傳輸、以公認標準程式加密後進行傳輸、或以符合電子簽章法之憑證加密後進行傳輸，以避免洩漏個人資料。

玖、資訊系統購置、發展及維護安全管理

三十七、　人體生物資料庫各項設備採購應依政府採購法規定辦理。

三十八、　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。

三十九、　人體生物資料庫資訊系統購置或維運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) 依照本院資訊室「第三方管理作業規範」等規定，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。

四十、 委外廠商服務異動時，應依本院「第三方管理作業規範」內容，考量下列因素並加以管理：

(一) 營運系統流程之重要性與重新評鑑之風險。

(二) 本院需評估項目：包括：變更供應商對本院之影響、評估尋找新委外廠商或自行開發應用程式與系統、網路管理上之變更、是否調整政策與程序、是否更新資安事件之控制程序等。

(三) 以上服務異動評估結果應提交本院人體生物資料庫倫理委員會審查

通過，並簽呈院部長官核示後執行，以避免資訊安全危機產生。

拾、資訊資產之管理

四十一、　人體生物資料庫各項設備採購應依政府採購法規定辦理，俟驗收完成後始得啟用。

四十二、　人體生物資料庫各項儲存設備報廢時，應核定其堪用狀況後，始得辦理報廢。

四十三、　人體生物資料庫各項儲存設備報廢時，應進行必要之資料清除作業，以避免內存資料外洩。

拾壹、實體及環境安全管理

四十四、　人體生物資料庫資訊處理設施所在區域應採取適當控制措施，以確保區域安全性，包括以下事項：

(一) 人體生物資料庫資訊設備應設有門禁管制，並保存於合於電腦機房安全空間。

(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，進出人員應經授權，並有安全管控措施。

(三) 人體生物資料庫系統機房應設置環境監控系統，可掌握機房溫、溼度狀況，並設置消防設備。

(四) 人體生物資料庫系統機房應設置不斷電系統，以確保供電穩定無虞。

四十五、　人體生物資料庫各項資訊設備移出設置者時，應經資訊安全管理主管人員之核定，始得放行。

四十六、　人體生物資料庫各項儲存設備報廢時，應核定其堪用狀況後，始得辦理報廢。

四十七、　辦公室桌面應依本院「資訊安全管理規定」辦理。重點如下：

(一) 使用電腦處理個人資料完畢即應清除畫面，不得將個人資料殘留於電腦終端機上。

(二) 個人電腦及終端機不使用時，應有關機、登出、或設定有密碼保護之螢幕保護程式或以其他控制措施進行保護。

(三) 公文及磁片長時間不使用及下班後應妥為存放，機密性、敏感性資訊應妥為收存。

(四) 棄置之手寫或影印公文廢紙及已過保存期限之公文，若為機密性、敏感性者，應依機密文件管理辦法予以銷毀。

拾貳、資訊安全事件發生之通報及保全處理程序

四十八、　當人體生物資料庫發生資訊安全事件時，臨床資訊登錄人員應立即

通報資訊室分機 2121 處理，並告知執行祕書。

四十九、　資訊室值班人員接獲通報後，應即刻通報人體生物資料庫資訊系統維運人員進行處理。人體生物資料庫資訊系統維運人員判斷事件等級，填寫「人體生物資料庫資安事件通報與處理記錄表」，並通知資訊主管。

五十、　資訊安全事件發生時，應依本院人體生物資料庫「資訊安全事件通報及保全處理程序書」進行處理，重點如下：

(一) 應就資訊安全事件發生原因、影響等級、可能影響範圍、可能損失、是否需要支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。

(二) 依資訊安全事件發生原因實施緊急應變處置，並持續監控與追蹤管制。

(三) 評估資訊安全事件對業務運作造成之衝擊，並進行損害管制。

(四) 若為本院無法處理事件，應通報上級主管機關輔導會或轉請「行政院國家資通安全會報」協助處理。

五十一、　資訊安全事件通報主管機關及通知參與者，應依本院人體生物資料庫「資訊安全事件通報及保全處理程序書」進行處理，重點如下：

(一)若發生人體生物資料庫相關資料、資訊遭竊取、洩漏、竄改或受其他侵害情事時，應於確認受侵害內容及可能影響範圍後，通報主管機關。

(二)前項受侵害內容及可能影響範圍應於查明後以書面、電話(簡訊)、電子郵件、或本院網站公告等方式通知相關參與者。

(三)參與者可依本院「人體生物資料庫--遭受侵害情事通報機制及救濟措施規範」，向本院請求救濟措施。

五十二、　資訊安全事件結束後，應依本院人體生物資料庫「資訊安全事件通報及保全處理程序書」進行處理，重點如下：

(一) 重大資安事件應填報「危機事件檢討紀錄表」，並提送本院「人體生物資料庫委員會」審查，以強化資訊安全防護機制

(二) 檢討可能發生危機因素，檢討預防方法及標準處理程序有效性，研擬預防方法或建立標準處理程序，列入後續定期執行項目。

五十三、　資訊安全事件通報及處理程序每年應進行檢討修正。

拾參、業務持續及回復管理

五十四、　應依照資訊室「資訊危機緊急應變計畫」，評估各種災害對人體生物資料庫業務運作之影響，訂定「人體生物資料庫緊急應變及回復作業程序」，並定期進行演練及檢討改善。

五十五、　每年應進行至少一次資訊安全風險評估，並據以修正人體生物資料庫資訊安全相關規定。

五十六、　人體生物資料庫之備份作業規劃及回復管理程序如下：

(一) 每週應進行備份作業至少一次，備份媒體應保存至少三代，備份媒體可循環使用。

(二) 備份媒體應至少存放一份於異地儲存，以確保備份媒體安全。

(三) 資料備份作業執行人員應於備份完成後填寫備份紀錄，註明備份結果。

(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。

五十七、 本院人體生物資料庫不提供國際傳輸服務。如有需要進行國際傳輸前，應擬訂相關規定及作業程序，提交本院人體生物資料庫倫理委員會審查通過，簽呈院部長官核示後公告實施。

拾肆、稽核管理

五十八、 人體生物資料庫應訂定年度資訊安全稽核計畫，並應視需要不定期進行專案稽核；稽核紀錄應永久保存且不允許更改。

五十九、 人體生物資料庫若提供第三人使用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，並準用前項規定，對該第三人進行資訊安全稽核。

六十、 前兩項稽核計畫、稽核報告結果及改善計畫，應送倫理委員會審查。倫理委員會得視必要，指派人員會同稽核。

拾伍、其他

六十一、 本規定及相關作業程序每年應進行檢討修正，提交本院人體生物資料庫倫理委員會審查通過，簽呈院部長官核示後公告實施，並報主管機關備查，修正時亦同。

六十二、 其他資訊安全規定事項悉依本院現有各類資訊安全管理規定辦理。