財團法人演譯基金會

美兆健康資源中心

美兆健康數據資料庫
資訊安全管理規範

技術報告編號：MJHRF-TR-03

2016/04/12

引用本文參考文獻格式：

莊淵傑(2016)。**美兆健康數據資料庫資訊安全管理規範**。財團法人演譯基金會技術報告(編號：MJHRF-TR-03)。

美兆健康數據資料庫資訊安全管理規範

一、 前言

美兆健康資源中心（以下簡稱本中心）所收集的資訊，無可避免的會涉及個人資料，所以在資料收集、整理與運用的過程中，我們除了依據行政院衛生福利部所頒訂的「人體生物資料庫資訊安全規範」（詳見附錄一）來管理相關資料，以及恪遵個人資料保護法的相關規定外，也參照國際資訊安全管理系統（ISO27001:2005），建立相關資訊安全制度，以保護資料提供者的個人資訊，並維護資訊系統的永續營運。

二、 資訊安全管理組織與人員管理訓練

為落實資訊安全管理制度，本中心成立資訊安全委員會，訂定保護個人資訊資產及執行特定資訊安全作業相關人員之責任與權限，透過資料管理組、生物醫學組、倫理委員會與稽核組的分工，達到督導、核定、協調與監督等機制，確保資訊安全政策之執行。

對於本中心之員工，會定期舉行資訊安全的教育、宣導及訓練，提高員工的資訊安全意識，瞭解最新的資安議題，並分享最新的相關法令規範，以提升本中心資訊安全的防護機制。對於新進員工，也需進行安全評估，並簽署機密維護合約，以明確告知人員之責任。

三、 資料之保護與運用

本中心對於個人資料之保存，採實體隔離方式作業，將資料存放於獨立之電腦主機，僅作為識別個人之用途，不會提供研究使用，個人資訊進入儲存系統後，就以代碼取代個人識別資訊，作為後續處理作業的依據，以減少個資暴露的風險；而健康問卷與生化數據資料的部份，當有研究分析運用的需求時，都需經過本中心相關部門或倫理委員會審查研究計畫後，才能提供去識別化的資料，為個人資料做最嚴格的防護。

對於重要的資料檔案依相關規定，以安全的方式保存與傳輸，在考量資料的機密性或敏感性後，採取適當的加密技術或交由可信賴的人員傳送，以防止遺失、毀壞、被偽造或竄改；另外，資料也會定期進行備份以及回復演練，以避免資料毀損，造成無法挽救的損失。

四、 資訊資產之管理

本中心已建立一份與資訊系統有關的資訊資產清冊，包含資產的項目、擁有者及安全等級分類等，並依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，建立資訊安全等級之分類標準，以及相對應的保護措施；在完成資產清冊後，依據每個資產之價值、威脅等級與弱點等級，進行風險評估，並針對高風險的項目，提出改善計畫，定期追蹤改善狀況，以降低任何危害資訊系統的可能。

五、 電腦系統安全管理

透過資訊系統作業程序文件，載明電腦系統相關作業程序的詳細規定，確保資訊系統之正確操作；另建立處理資訊安全事件之作業程序與紀錄，並課予相關人員必要的責任，以便迅速有效處理健康資源中心資訊安全事件。

對於資訊系統的維護，本中心隨時注意分析系統的作業容量，以避免容量不足而導致電腦當機，並觀察分析系統資源使用狀況，包括處理器、主儲存裝置、檔案儲存等系統之使用趨勢，尤應注意系統在業務處理及資訊管理上的應用情形。若有開發新系統之需求，應依照相關作業標準，在上線作業前，執行適當的測試，以驗證系統功能符合既定的標準。

六、 結語

面對科技的日新月異，數位資料取得變得容易，也相對的增加資料洩漏的風險，唯有不斷的瞭解與更新資訊安全的相關知識與技術，才能提供可靠的個人資料保護，本中心透過資訊安全組織的建立、規劃、執行與稽核，由上而下貫徹資料保護的信念與決心，務必給予會員個人資料最完善的保護。

附錄一　人體生物資料庫資訊安全規範

法規名稱：人體生物資料庫資訊安全規範

訂定時間：中華民國 099 年 07 月 02 日

一、設置者訂定之資訊安全管理規定（以下稱資安規定），應包括下列事項：

（一）資訊管理單位之組織、權責及分工。

（二）人員管理及資訊安全訓練。

（三）電腦系統安全管理。

（四）網路安全管理。

（五）資訊系統存取控制管理。

（六）資訊系統購置、發展及維護安全管理。

（七）資訊資產之管理。

（八）實體及環境安全管理。

（九）資訊安全事件發生之通報及保全處理程序。

（十）業務持續及回復管理。

（十一）本規範與相關法令規定事項，及其他有關資訊安全事項。

資安規定應經設置者之倫理委員會審查通過後，報主管機關備查，修正時亦同；倫理委員會審查時，應有資訊安全專家參與。資安規定應逐年檢討，並為必要之修正。

二、設置者應指定主管人員負責資訊安全管理事項之協調及推動，並得成立資訊安全推行小組，辦理資訊安全政策、規劃、執行等審議、督導事項。

三、設置者對資訊有關業務及人員，應進行安全評估。

四、設置者應依所屬人員之業務特性，定期辦理資訊安全教育。

五、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間，不得互為兼任。

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；該專人不得兼任前項相關資料、資訊之管理人員。

六、設置者得將資訊業務委託其他廠商辦理，應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。

七、設置者應定期更新漏洞、電腦病毒碼及其他惡意軟體防範之程式，確保應用系統正常運作。

八、收案後所建置之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。

九、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。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。

十、設置者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。

十一、設置者所屬人員之系統存取權限，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。

十二、設置者離（休）職人員，應立即取消使用設置者各項資訊資源之所有權限，並列入離（休）職之必要手續。

十三、設置者應建立系統使用者註冊管理制度，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，由設置者視運用系統及安全管理需求決定，最長以六個月為限。

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。

資訊之存取紀錄，應保留一定期間，並限制紀錄之存取活動，以維持其完整性。

十四、設置者對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，應在設置者所屬人員監督下為之。

十五、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。

十六、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。

各項儲存設備報廢時，應核定其堪用狀況後，始得辦理報廢。

發現有不明人士，未經許可擅接網路之情事，應立即通知。

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。

十七、設置者為辦理人體生物資料庫管理條例（以下簡稱本條例）第十一條第一項所定之事宜，應事前擬訂建立資訊安全事件通報機制，作成事件處理紀錄，並應供日後教育訓練學習使用，且併同本條例第十一條第二項關於救濟措施之規範報主管機關核定。

十八、設置者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。

設置者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。

前二項之稽核計畫、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。