2011 年 11 月 25 日訂定
2023 年 07 月 24 日修訂
2023 年 07 月 24 日檢視

人體生物資料庫
資訊安全管理辦法

編號：M2-066-A

版次：第十一版

1. 總則

1.1 目的

強化義大醫療財團法人義大醫院(以下簡稱本院)之人體生物資料庫(以下簡稱本庫)資訊安全管理，建立安全及可信賴之電子化系統，確保資料、系統、設備及網路之安全並保護受試者之隱私，依衛福部「人體生物資料庫管理條例」及「人體生物資料庫資訊安全規範」，特訂定「M2-066-A 人體生物資料庫資訊安全管理辦法」(以下簡稱本辦法)。

1.2 適用範圍

適用於資料庫施作範圍內之資訊安全事件管理。

1.3 負責單位

本辦法由人體生物資料庫制定、修訂及廢止，經「AFO-021 人體生物資料庫倫理委員會」(以下簡稱本委員會)審議通過，呈核准後實施。

1.4 管理單位

本辦法由醫務管理室發行、登記及保存。

2. 資訊安全管理辦法

2.1 權責單位

2.1.1 資訊主管：由本院資訊單位主管擔任。

負責督導、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之責，並執行解密作業。

2.1.2 專責資訊人員(含資安維護人員、資訊系統開發人員及資料庫管理人員)：

(1) 管理內部資訊硬體、軟體設備。

(2) 管理本庫所有資訊、資料、電子檔案。

(3) 管理本庫對外網頁。

(4) 訂定年度稽核計畫。

2.1.3 生物醫學主管:執行解密作業。

2.1.4 資料處理人員(本庫資料人員):管理參與者資料及參與者同意書。

2.1.5 檢體處理人員(本庫檢體人員):管理參與者檢體。

2.2 作業內容

2.2.1 本庫施作範圍內之人員皆須簽署「IS-D-013 保密切結書」，不得洩漏參與者隱私。

2.2.2 本庫所有檢體於儲存及登錄時皆進行編碼，單從檢體管子上無法辨識檢體之所有人。

2.2.3 參與者姓名、身分證及出生年月日等可辨識之個人資料之資訊及文件，予以加密並單獨管理。若有需解密之情事，需由本委員會同意方得解密。

2.3 作業要求

2.3.1 人員管理及資訊安全訓練

(1) 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，不得互相兼任。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。

(2) 本庫專責資訊人員進用、工作及任務指派時，應依「資訊人員職掌清冊」審慎評估人員之適任性。

(3) 各工作角色所負責之各項工作應訂定該項工作之職務代理，職務代理之指派仍須符合權責區隔之原則。

(4) 人員離(休)職時，應取消其進出識別證件，及各項資訊、資源之所有權限，並列入離(休)職之必要手續，並確實做好電腦軟硬體及相關文件之移交工作。

(5) 專責資訊人員、資料處理及檢體處理人員每年應接受本院所舉辦之資訊安全教育訓練 3 小時。

2.3.2 電腦系統安全管理

(1) 辦理資訊業務委外作業時，應依據「IS-B-010 委外管理程序書」之作業說明規定辦理；委外廠商服務異動的管理程序，依據「IS-B-010 委外管理程序書」之服務變更管理規定。

(2) 電腦系統作業變更時，應至 MIS 詳實填寫「電腦作業需求單」，並交由主管核可。

(3) 依相關法規或契約規定，複製及使用軟體；嚴禁使用非法軟體。

(4) 電腦系統中須裝置防毒軟體，以防止感染電腦病毒，並定期更新漏洞、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。

(5) 每年定期辦理資訊安全內部稽核作業，並視需要不定期執行專案稽核。稽核前，先將資訊安全稽核計畫填寫於「IS-D-040 資訊安全管理制度內部稽核計畫」，並依據「IS-D-041 資訊安全管理制度內部稽核表」之標準作業程序進行稽核。

(6) 資訊安全內部稽核作業之稽核紀錄將永久保存。

2.3.3 網路安全管理

(1) 本庫之管理，區分為『參與者資料』與『參與者檢體』二個獨立的管理系統，操作權限上亦分屬於此二位不同之管理者，且單一管理者僅具備存取一種資料的權限，以確保資料的安全與保密性。

(2) 收案後所建置之生物資料庫之個人資料，應以實體隔離方式建構及使用，其資訊系統不得與網際網路連接。

(3) 為提升作業之安全性，依據「IS-B-007 通信與作業管理程序書」之電腦管理及安全防護規定，應視需要使用加密通道（如 VPN、SSH）等各種安全控管技術。

(4) 利用網路公佈及流通資訊時，應評估資料安全等級，機密、敏感性或未經當事人同意之個人隱私資料及文件，不得上網公佈。

(5) 本庫有關資訊，非經本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。經本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。出庫資料一律加密並燒成光碟後釋出。

(6) 資訊系統安全控管機制及網路控制措施，依據「IS-B-007 通信與作業管理程序書」之相關規定辦理。

2.3.4 資訊系統存取控制

(1) 本庫所屬人員之系統存取權限，以執行其職務所必要者為限。資料庫及檔案應建立機密及安全等級管理制度。應按不同業務範圍及使用權限，分別設定服務功能、密碼。須輸入生物資料庫人員之帳號及密碼，經驗證通過後，方可登入人體生物資料庫資訊系統，但僅限存取使用該人員業務範圍及權限之資訊系統功能與服務。

(2) 依據「IS-B-008 存取控制管理程序書」規定，使用者之密碼設置至少 6 碼，且應符合密碼設置原則，如參雜數字、英文字母、特殊符號、大小寫，使用者應至少 3 個月更換密碼一次，並禁止重複使用相同的密碼。相關系統存取權限經由本委員會授權核發予最高權限人員-人體生物資料庫倫理委員會主席及人體生物資料庫代表人。如申請或變動存取權限，應填妥「資訊系統存取權限申請表」，經上述最高權限人員核准後，送交資訊單位建立使用者系統存取帳號。

(3) 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週期。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資訊操作日誌。

(4) 依據「IS-B-008 存取控制管理程序書」規定，使用者存取權限應定期審查，週期不得超過 1 年。

(5) 依據「IS-B-008 存取控制管理程序書」規定，所有資訊資源使用者，非經最高權限之人員授權或允許，禁止執行遠端存取作業。

(6) 行動電腦(如筆記型電腦、隨身碟)內之資料內容如不再需要，應確實清除。如欲把行動電腦攜出本庫，需填妥「資訊系統存取權限申請表」，並得到最高權限人員之核准授權，且保留所有攜出記錄以維護稽核存底。

(7) 各項正式作業之電腦系統操作及資料處理，須指定專人負責建檔、核對、更新、審查及維護電腦資料之正確性。資訊系統開

發人員非經核准不得操作使用或更改已正式作業之系統檔案。

(8) 資訊之存取紀錄，應保留三年，並限制紀錄之存取活動，以維持其完整性。

(9) 若遇下列事件得請資料處理人員填寫「資料解密申請表」，經本委員會主席或執行秘書書面同意，由人體生物資料庫代表人、生物醫學主管及資訊主管中任兩位主管於同一天進行解密，待該資料使用完畢，由上述主管中任一位主管予以銷毀該資料，相關執行解密及銷毀作業皆需於「資料解密申請表」及「資訊操作日誌」上簽名，並呈報本委員會備查，以完成解密執行程序:

(a) 經主席或執行秘書書面同意之參與者退出案及實地查核作業。

(b) 經本委員會書審程序通過之國家級整合平台出庫申請案及加值服務申請案。

(c) 經書審及本委員會會議通過之本院出庫申請案。

2.3.5 系統發展及維護安全管理

(1) 自行開發或委外發展之系統，應在系統之初始階段即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動等作業，應予安全管制，避免不當軟體及電腦病毒危害系統安全。

(2) 資訊系統之軟體安裝、測試、上線、驗收程序，依據「IS-B-009 系統開發與維護程序書」規定辦理。

(3) 委託廠商建置及維護重要軟硬體設施時，應在本單位相關人員監督及陪同下始得為之。

(4) 對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，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；並將本程序書納入成為契約之一部分，並嚴禁核發超過三個月之系統辨識碼及通行密碼；基於實際作業需要，得核發短期性及臨時性之系統辨識與通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

(5) 各項儲存設備報廢時，依據「IS-B-006 實體安全管理程序書」之一般設備安全規定，確實清除設備資訊，方可進行報廢，應

避免內存資料外洩。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。

2.3.6 資訊資產安全管理

(1) 對於儲存各項機密資料或程式軟體之光碟片及報表等媒體，應設專人管理並定期備份，並存於上鎖之儲存櫃中，防止資料洩漏或毀損，資料備份情況應記錄於資訊操作日誌當中，並將備份後的光碟片送至育成研究大樓進行異地保存。

(2) 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。

2.3.7 實體及安全環境管理

(1) 為確保相關設施之安全，依據「IS-B-006 實體安全管理程序書」之安全區域規定，非管理單位指定之人員不得擅自進入安全區域或使用相關資訊設備，只有授權人員，可以進出安全區域。本庫之安全區域為存放含參與者個人資料、資訊之電腦設備、文件之空間，此資料室具門禁鎖，人員進出此區域皆需管制，僅限本庫資料人員、檢體人員及其職務代理人進出，以外人員進出，均須於「人員進出資料室登記表」登記後，由本庫資料人員或檢體人員或職務代理人陪同進入資料室。

(2) 對於電腦設備之裝置地點，應考量使用及管理上之安全，並應指定專人負責管理。管理或使用人員應詳細記載電腦設備故障、異常及維護等情形，以做為設備更新及作業安全之依據。

(3) 電腦設備應保存於可上鎖的安全空間內並採用適當實體保護措施，防止火災、地震及其他自然或人為災難的損害。

(4) 為防止文件及儲存媒體遭未經授權人員取用，依據「IS-B-006 實體安全管理程序書」之一般控制措施規定，同仁應於離開本單位，遵守桌面淨空政策，並將含個資之文件與可攜式資訊設備皆存放於儲存櫃並上鎖，避免資訊外洩。

(5) 應設計不斷電系統備援電力措施，以有效維持本庫生物資訊系

統相關主機與網路設備之持續服務性。

(6) 本庫各項資訊設備移出原設備放置空間時，應經資訊主管之核定，始可放行。各項儲存設備報廢時，應核定其堪用狀況後，始得辦理報廢。

2.3.8 資訊安全事件發生之通報及保全處理程序

(1) 本庫人員遇有任何資訊安全之可疑情形，應立即向本庫資訊安全維護人員通報，以採取適當反應措施。

(2) 資訊安全事件發生之通報標準作業程序，依據「IS-B-011 安全事件管理程序書」之通報程序規定辦理。

(3) 當發現異常事件無法在 30 分鐘內處理完畢時，應由本庫資訊安全維護人員通報資訊單位相關人員處理。

2.3.9 業務持續及回復之管理規定-依據「IS-B-012 業務運作永續管理程序書」之規定，確保本庫業務永續運作，並降低關鍵性業務流程受重大故障或災害之影響。每半年進行一次弱點掃描，並將弱點掃描之紀錄備存。

2.4 未盡事宜，依院內資訊單位發布之資訊安全管理程序書執行，修改時亦同。

3.附件

3.1 IS-B-006 實體安全管理程序書
3.2 IS-B-007 通訊與作業管理程序書
3.3 IS-B-008 存取控制管理程序書
3.4 IS-B-009 系統開發與維護程序書
3.5 IS-B-010 委外管理程序書
3.6 IS-B-011 安全事件管理程序書
3.7 IS-D-040 資訊安全管理制度內部稽核計畫
3.8 IS-B-012 業務運作永續管理程序書

4.附則

4.1 修訂紀要

4.1.1 2011 年 11 月 25 日新設第一版。

4.1.2 2012 年 07 月 12 日修訂第二版。

4.1.3 2013 年 04 月 18 日修訂第三版，修訂重點:

(1) 內文名詞修改。

(2) 修訂「IS-D-041 資訊安全管理制度內部稽核表」及「資訊系統存取權限申請表」。

(3) 年度修改為西元年。

4.1.4 2013 年 12 月 02 日修訂第四版，修訂重點:

(1) 修改條文:2.2.1 及 2.3.5。

(2) 刪除 3.表單。

4.1.5 2014 年 11 月 07 日修訂第五版，修訂重點:

(1) 修改條文:1.4 管理單位

4.1.6 2016 年 02 月 04 日修訂第六版，修訂重點:

(1) 修改條文:辦法名稱

(2) 修改條文:1.1 目的

(3) 修改條文:2.2.1 資訊主管。

(4) 修改條文:2.3.4 資訊系統存取控制之(1)

(5) 修改條文:2.3.8(3)

4.1.7 2017 年 12 月 01 日修訂第七版，修訂重點:

(1) 修改條文: 2.1 權責單位之 2.1.2 專責資訊人員

(2) 修改條文: 2.3.4 資訊系統存取控制之(3)

(3) 修改條文: 2.3.5 系統發展及維護安全管理之(5)

(4) 修改條文: 2.3.6 資訊資產安全管理之(1)

(5) 修改條文: 2.3.9

4.1.8 2018 年 11 月 12 日修訂第八版，修訂重點:

(1) 修改條文: 2.1.2 專案資訊人員改為專責資訊人員

(2) 修改條文: 2.3.1 人員管理及資訊安全訓練(5)

(3) 新增條文: 2.3.4 資訊系統存取控制(9)

(4) 修改條文: 2.3.6 資訊資產安全管理(1)

4.1.9 2019 年 09 月 16 日修訂第九版，修訂重點:

(1) 修改條文: 1.3 及 1.4

(2) 修改條文: 2.3.1 人員管理及資訊安全訓練(5)

(3) 修改條文: 2.3.4 資訊系統存取控制(1)及(9)

(4) 修改條文: 2.3.6 資訊資產安全管理(1)

(5) 修改條文: 2.3.7 實體及安全環境管理(1)及(4)及(6)

(6) 修改條文: 2.3.8 資訊安全事件發生之通報及保全處理程序(1)及(3)

4.1.10 2020 年 11 月 27 日經檢視不修訂。

4.1.11 2021 年 10 月 18 日經檢視不修訂。

4.1.12 2022 年 03 月 08 日修訂第十版，修訂重點:

(1) 修改條文:2.1.1 資訊主管

(2) 新增條文:2.1.3 生物醫學主管

(3) 修改條文:2.3.3 網路安全管理(5)

(4) 修改條文: 2.3.4 資訊系統存取控制(7)&(9)

4.1.13 2023 年 07 月 24 日修訂第十一版，修訂重點:

(1) 修改條文:2.3.4 資訊系統存取控制(9)