1. 目的：佛教慈濟醫療財團法人大林慈濟醫院(下稱本院)人體生物資料庫(下稱本生物資料庫)為確保本生物資料庫之資訊作業符合法規，特依據衛生福利部公告之「人體生物資料庫資訊安全管理規範」訂定「佛教慈濟醫療財團法人大林慈濟醫院人體生物資料庫資訊安全管理規則」。

2. 適用範圍：所有可能接觸本生物資料庫參與者資訊之人員。

3. 定義：保護本生物資料庫參與者的個資，避免洩漏、竊取與竄改等情事發生，並確保本生物資料庫之資訊作業符合法規與資訊安全。

4. 相關文件：

4.1 衛生福利部「人體生物資料庫資訊安全管理規範」。

5. 作業說明：

5.1 管理單位的組織與任務

5.1.1 本生物資料庫－負責資訊安全管理事項之協調及推動。

5.1.2 資訊主管－負責制定資訊安全政策及資訊安全管理規則。

5.1.3 資訊人員－負責硬體系統與資訊之管理，落實執行資訊安全管理規則。

5.1.4 本生物資料庫之所有成員：遵循資訊安全管理規則落實於工作中。

5.2 人員管理

5.2.1 執行資訊有關業務之人員招募與錄用時應進行適性評估（如資訊能力資安概念、操守、歷任任職紀錄等）；資訊人員則由資訊主管協助評估、安排與管理。

5.2.2 本生物資料庫資訊系統之維護，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，每六個月須更換一次；承作者執行維護作業，將在管理者所屬人員監督下為之。

5.2.3 本生物資料庫之資訊管理人員不得為研究人員，反之，使用本生物資料庫檢體與資料之研究人員亦不得兼任資訊管理人員。

5.3 安全訓練

5.3.1 依循資通安全管理法，所有成員（包含主管與組員）每年必須接受三小時以上一般資通安全通識之教育訓練課程。

5.3.2 資安教育訓練課程可採現場或線上數位課程方式辦理。

5.4 電腦系統安全管理

5.4.1 本生物資料庫電腦設備及主機須依照本生物資料庫「資安手冊」規定進行安全與維護措施。

5.4.2 系統主機應設於有門禁與監視器監控之環境，進出人員應有安全管制措施，資訊人員依負責業務取得使用帳號密碼，不得外洩。

5.4.3 電腦開機需設定密碼，並記錄各項存取、修改、刪除。

5.4.4 電腦不使用時，應予關機、登出、設定螢幕密碼或是以其他控制措施保護。

5.4 5 各項重要之作業系統、應用軟體及相關檔案等資料，均應製作備份；使用防火、防震等保險設備異地存放。有關電腦程式及其設計、測試、製作、使用及維護，均應嚴密管制，核定使用之程式不得擅自變更，其有變更之必要時應報請主管經核准後為之。

5.4.6 資訊人員安裝軟體或更新資料庫程式及病毒掃瞄作業時，可使用筆記型電腦、光碟片、隨身碟等可攜式儲存媒體協助作業，作業時須有行政人員或資訊主管陪同作業。

5.4.7 系統主機應定期進行系統病毒掃瞄作業和修補系統漏洞。

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

5.5 網路安全管理

5.5.1 本生物資料庫的系統主機不與網路系統相連，收案後所建置之生物資料庫之個人

資料，以實體隔離之方式建構及使用，並與院內及院外網路完全隔絕。

5.5.2 有關個人資料的資訊不在單位間交換，若因業務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。

5.5.3 有關個資之機密資訊，非經本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。經本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。

5.6 資訊系統存取控制管理

5.6.1 本生物資料庫人員對資訊系統存取的授權以執行其職務所必要者為限，以符合最小權限原則。授權經本生物資料庫資訊主管或代理人審查通過後，以書面、電子或其他方式告知工作人員相關之權限及責任。

5.6.2 建立有權限進入資訊系統的人員名冊，於填寫「帳號申請表格」後，經註冊申請程序後始可獲得系統使用權限。

5.6.3 使用者應於權限申請核准後首次登錄系統時，依密碼設定原則立即修改預設密碼，密碼設定的原則為至少八碼並須為數字與英文字母混合。密碼須妥善保管，避免他人知悉。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。

5.6.4 管理人員存取、增刪、查閱、複製本生物資料庫記錄時，資訊系統應將執行人員、操作行為與時間等資料加以記錄且定期執行備份作業，此記錄應設定為唯讀資料並保存三年以利後續查核之用。各系統記錄僅能由系統管理者及具讀取權限者查閱。

5.6.5 工作人員於每次進入放置實體隔離之電腦的行政辦公室並處理各項資料時，應記錄進入進出的時間、攜入、攜出的物品、與所從事之活動。每年由本生物資料庫倫理委員會主任委員指派專家或委員查核本生物資料庫所屬人員之系統存取權限及活動日誌。

5.6.6 處理個人資料加解密業務時，所有電子文書作業應於實體隔離之電腦上處理，不

得進行遠距操作，並將檔案存放於專屬資料夾，此電腦設備僅提供個案資料管理者與金鑰管理人員使用，電腦使用完畢後應立即登出。資料列印後應立即將文件收妥，以免資料外洩。實體隔離環境下之個人電腦及印表機，不得移作其它用途。

5.6.7 資料庫以行動硬碟進行資料庫的備份，以光碟片使用於資料庫的入出庫管理。

5.6.8 本生物資料庫各項資料與資訊之安全措施依參與者之同意範圍不同，進行不同等級之保護，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。

5.6.9 離（休）職人員，立即取消使用設置者各項資訊資源之所有權限。

5.6.10 本生物資料庫應不定時備份，備份的媒體應加密保護，且須採異地儲存，以維護本生物資料庫的資訊安全無虞。

5.6.11 備份儲存的媒體，應不定時演練「資料還原」作業，以確保需要時可完整的還原。

5.7 資訊系統購置、發展及維護安全管理

5.7.1 本生物資料庫所使用之資訊系統由花蓮慈濟醫院資訊室開發，本院資訊室維護，若將來因需求必須將資訊業務委託其他廠商或學界專家辦理，須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；並將本規則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。

5.7.2 資訊設備於耐用期限屆滿或符合報廢條件時，由資訊人員及資訊主管共同確認所報廢之資訊設備內的資訊已完全被刪除及儲存媒體實體破壞後，始得進行報廢處理，留存紀錄備查。

5.7.3 本生物資料庫所屬之資訊設備與軟體不得在未經資訊主管或代理人的授權下移出本生物資料庫或修改。

5.8 實體及環境安全管理

5.8.1 本生物資料庫資訊設備之安置與人員進出之管制須依照本生物資料庫設置書、「資安手冊」與本生物資料庫管理辦法進行。

5.8.2 處理本生物資料庫資料的電腦置於實體隔離的辦公室內，重要資訊設備應裝置於管制區域內，實體隔離的辦公室與管制區域皆設有門禁，並依權限管制人員進出，以避免未經授權存取系統的機會。

5.8.3 管制區域內應設置適當的環境監控設施以監控環境的變化及人員的行為，並應設置安全防護設備，如：消防設備，以確保資訊安全事故發生時能夠及時處理，避免事態擴大，平時應進行安全訓練以確保工作人員對緊急事件的應變能力。

5.8.4 資訊設備安置時，應檢查及評估火災、漏水、地震、電力供應等可能的風險。當發生天然災害、網路入侵或主機異常導致系統無法正常運作時，發現人依事故歸屬通報權責單位並通知直屬主管，由資訊人員及行政人員進行系統損害程度評估與回復作業。

5.8.5 資料或資訊遭竊取、洩漏、竄改或受其他侵害情事時，依本生物資料庫的「參與者權利救濟通報機制及救濟措施規範」處理之。

5.8.6 電腦設備之設置應予以保護，防止斷電或其他電力不正常所導致的傷害，重要資訊設備應考量安置預備電源或使用不斷電系統；設備的維護作業應予以紀錄並留存，以為日後稽核之參考。

5.8.7 特殊性、機密性、敏感性文件及資訊儲存媒體長時間不使用及下班後，應妥為存放，棄置之手寫或影印公文廢紙及已過保存期限之公文，應視需要予以銷毀，工作時，只取用所需資料，桌面應儘量保持淨空狀態。

5.9 資訊安全事件發生之通報及保全處理程序

5.9.1 本生物資料庫資訊安全事件發生之通報及保全處理程序依據本生物資料庫「資安手冊」辦理。

5.9.2 當發生資訊安全事件時，行政人員應立即通報資訊室處理，並告知資訊主管。資訊室接獲通報後，應及時通報本生物資料庫資訊人員進行處理。依據進行系統損害程度評估，並通知主管。

5.9.3 若發生本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。

5.9.4 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) 或電子郵件等方式通知相關參與者。

5.9.5 參與者可依本院「參與者權利救濟通報機制及救濟措施規範」，向本院請求救濟措施。

5.9.6 資訊安全事件處理結束後，依應變回復計畫，實施災後復原重建，以恢復系統正常運作。

5.9.7 重大資安事件應立即通報主管機關，並提送本院「資通發展暨安全管理委員會」審查，以強化資訊安全防護機制。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。

5.9.8 資訊安全事件通報及處理程序應每年進行檢討修正，並將資訊安全事件處理流程作成紀錄供日後教育訓練學習使用。並由本生物資料庫倫理委員會主任委員指派專家或委員每年稽核一次資訊與資料的安全性，稽核紀錄應永久保存。

5.10 業務持續及回復管理

5.10.1 依照本生物資料庫「資安手冊」，評估各種災害對本生物資料庫業務運作之影響，定期進行演練及檢討改善。

5.10.2 本生物資料庫之備份作業規劃及回復管理程序如下：每次變動應進行備份作業至少一次，備份媒體可循環使用。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。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。

5.10.3 不定期進行備份媒體回復測試作業。作業程序如下：倒回最近一次備份資料；實施資料完整性檢查；測試系統是否可正常作業。

5.10.4 回復測試作業由資訊人員執行，並會同行政人員於回復完成後填寫回復測試紀錄，註記回復測試結果。

5.10.5 備份作業流程及回復測試流程應每年進行檢討修正。

5.10.6 本生物資料庫依據「人體生物資料庫資料國際傳輸或生物檢體衍生物輸出審查標準」，經過衛福部審查通過後，可進行跨國合作。

5.11 修訂

5.11.1 本規則經本生物資料庫倫理委員會審查通過後，報主管機關備查，修正時亦同。

本規則應定期檢討，並為必要之修正。

6. 應用表單：無