高雄醫學大學

個人資料檔案安全維護計畫

機密等級：一般

文件編號：**PIMS-A-002**

版　　次：**1.1**

發行日期：**109/10/23**

修 訂 紀 錄				
版次	**修訂日期**	**修訂頁次**	**修訂者**	**修訂內容摘要**
1.0	108/1/29		謝志昌	初版
1.1	109/10/23	p.4~p.5 p.17	謝志昌	增加: 5.1 組織全景 5.12 個人資料保護管理目標與績效評估 修改: 5.2.3【稽核室主任】改為【圖書資訊長】

目錄

1 目的 3

2 適用範圍 3

3 權責 3

4 名詞定義 3

5 作業說明 4

1 目的

高雄醫學大學(以下簡稱本校) 為確保個人資料檔案管理之安全，並強化對個人資料之保護能力，防止個資外洩事件發生，達成持續改善之目標，特制定本計畫。

2 適用範圍

本校承辦相關個人資料作業均適用之。

3 權責

3.1 資訊安全長

3.1.1 核定個人資料檔案安全維護計畫

3.2 資訊安全委員會

3.2.1 審查個人資料檔案安全維護計畫

3.3 個人資料保護管理執行小組

3.3.1 研議個人資料檔案安全維護計畫

4 名詞定義

4.1 特種個資：依據個人資料保護法第 6 條，有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。特種個資除有個人資料保護法第 6 條第 1 項各款之情形，不得蒐集、處理或利用。

4.2 當事人權利：依據個人資料保護法第 3 條，個人資料之當事人對於其本身之個人資料可行使請求查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理、利用、請求刪除等權利。

4.3 跨單位個人資料檔案：個人資料檔案儲存於本校集中控管之資料庫，且該個人資料檔案係由本校多個單位蒐集與處理，並供全校多個單位對於該個人資料檔案進行合於特定目的之利用。

4.4 單一單位個人資料檔案：個人資料檔案未儲存於本校集中控管之資料庫，係以紙本或電子檔儲存於本校特定單位之辦公場所、儲存裝置或個人電腦，且該個人資料檔案係由本校同一個單位蒐集與處理，並供該單位對於該個人資料檔案進行合於特定目的之利用。

4.5 國際傳輸：指將個人資料作跨國（境）之處理或利用。

5 作業說明

5.1 組織全景

5.1.1 本校應鑑別內外部環境議題包括相關法令要求、行政院及教育主管機關所下達之重要決定或指導(包括但不限於主管機關之行政指導、重要會議決議事項)、本校透過相關會議所做成之決議(包括但不限於主管會報、行政會議或校務會議等之決議)等，針對個人資料安全之維護需求進行評估，並據此建立或調整範圍與目標。

5.1.2 本校應鑑別個人資料安全管理關注方(利害相關團體)與要求事項並留存文件化紀錄。

5.1.3 上述內外部環境議題與關注方要求之鑑別方式，請參閱「個人資料

保護管理組織程序書」。

5.2 個人資料保護管理組織

5.2.1 本校為落實資訊安全與個人資料之保護與管理、推動校園保護智慧財產權工作，設置「資訊安全委員會」，並由副校長一人擔任召集人並兼任「資訊安全長」。並於「資訊安全委員會」下設置「個人資料保護管理執行小組」。有關資訊安全委員會之組成、任務與權責，依「資訊安全委員會設置辦法」之規定。

5.2.2 本校之個人資料管理人由資訊安全長擔任。

5.2.3 本校之個人資料稽核人員由本校稽核室及圖書資訊處推派人員組成稽核小組，稽核小組組長由圖書資訊長指定成員擔任之。

5.2.4 有關個人資料稽核小組與個人資料保護管理執行小組之組成、任務與權責，另訂「個人資料保護管理組織程序書」規範之。

5.3 個人資料檔案盤點

5.3.1 本校蒐集、處理與利用個人資料之各單位，應定期清查所保有之個人資料檔案現況，並依照共通之格式彙整為個人資料檔案清冊。經定期檢視，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集處理或利用等適當之處置。

5.3.2 個人資料檔案之清查活動由個人資料保護管理執行小組發動，每年至少執行一次，並由個人資料保護管理執行小組統籌個人資料檔案清冊格式之維護與彙整。

5.3.3 用於進行清查之個人資料檔案清冊,應至少包括個人資料檔案名稱、個人資料檔案參考說明、法規依據、特定目的、類別、鑑別蒐集處理與利用流程及參與單位。用於發行或供本校各單位查詢之個人資料檔案清冊,由個人資料保護管理執行小組規劃適當之格式與內容,並採取必要保護措施，以避免個人資料檔案清冊遭未經授權之修改或誤用個人資料檔案清冊版本。

5.3.4 有關個人資料檔案清冊之清查、彙整與維護，另訂「個人資料檔案盤點管理程序書」規範之。

5.4 個人資料保護風險評鑑與風險管理

5.4.1 本校蒐集、處理與利用個人資料之各單位，應定期對於個人資料檔案於蒐集、處理與利用流程中可能發生之機密性、完整性、可用性與遵循性風險，進行風險鑑別、風險分析與風險評估等風險評鑑工作，並依據風險評鑑結果，對於高風險項目(風險等級 3)進行風險管理工作包括規劃適當控制措施、實作所規劃之控制措施與評估控制措施成效。

5.4.2 有關個人資料保護風險評鑑與風險管理之實施方式，另訂「個人資

料保護風險評鑑與管理程序書」規範之。

5.5 個人資料事故之預防、通報及應變機制

5.5.1 本校所屬人員於個人資料之蒐集、處理與利用流程，發生個人資料被竊取、竄改、毀損、滅失、洩漏或其他違反法規要求安全事故時，應向本校個人資料保護管理執行小組通報，或利用個人資料保護聯絡信箱進行通報。

5.5.2 個人資料保護管理執行小組於知悉可能之個人資料安全事故時，除依照其他規定例如資訊安全事件通報處理程序進行通報與處理外，應儘速完成個人資料事故進行受影響當事人數量、受影響個人資料檔案、引起訴訟可能性以及對當事人權益影響等評估，並採取處理措施包括查明個人資料事故發生原因、鑑別可行之緊急應變、損害抑制與證據保全措施等。並依照事故等級向上或向外通報。

5.5.3 個人資料保護管理執行小組與查明個人資料事故發生原因，應與發生事故權責單位共同規劃以適當方式包括言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或網頁資訊通知當事人。

5.5.4 有關個人資料安全事故之通報與處理方式，另訂「個人資料安全事故管理程序書」規範之。

5.6 當事人權利行使

5.6.1 本校個人資料檔案清冊中所列之各項個人資料檔案，依法接受個人

資料當事人行使當事人權利包括：請求查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理、利用、請求刪除等權利。

5.6.2 本校各單位於受理個人資料當事人行使當事人權利案件時，應先確認提出請求者為個人資料當事人本人，或經本人委託之代理人並有證明文件，方可受理該案件，並依處理期限規定回覆本人或代理人。

5.6.3 本校各單位於受理個人資料當事人行使當事人權利案件處理期限如下：

5.6.3.1 查詢、提供閱覽或製給複製本之案件：最長應於 15 日內，為准駁之決定；必要時，得予延長，延長之期間不得逾 15 日，並應將其原因以書面通知請求人。

5.6.3.2 請求補充或更正、請求停止蒐集、處理、利用、請求刪除之案件：最長應於 30 日內，為准駁之決定；必要時，得予延長，延長之期間不得逾 30 日，並應將其原因以書面通知請求人。

5.6.4 本校各單位應依據業務職掌，對於經常性之個人資料查詢或請求閱覽、請求製給複製本個人資料，規劃受理當事人申請行使上述各項權利之適當管道，並提供申請方式與收取費用之說明。

5.6.5 本校各單位接獲個人資料當事人請求停止蒐集、處理與利用、刪除或申訴時，應透過本校全球資訊網首頁所列個資保護聯絡窗口，請

求個人資料保護管理執行小組協助辦理。

5.6.6 個資保護聯絡窗口受理之案件，應保存完整之案件處理紀錄，記錄內容應顯示各個處理步驟之日期、時間、人員、動作與結果。

5.6.7 有關個資保護聯絡窗口受理各項案件之處理方式，另訂「個人資料當事人權利行使案件管理程序書」規範之。

5.7 個人資料蒐集、處理及利用

5.7.1 告知事項

5.7.1.1 除依法可免為告知之情形外，本校各單位應於以本校名義蒐集個人資料前，履行個人資料保護法第 8 條規定之告知義務，並應以當事人可瞭解之語言或方式,明確告知當事人以下事項:

1. 本校之名稱。
2. 蒐集之目的。
3. 個人資料之類別。
4. 個人資料利用之期間、地區、對象及方式。
5. 當事人依法得行使之當事人權利及方式。
6. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

5.7.2 單一單位個人資料檔案之蒐集，由各單位應指派專人研擬告知事項

內容，並由該單位主管核准後，作為對當事人告知之依據。跨單位個人資料檔案之蒐集，由蒐集單位研擬告知事項內容，並由個人資料保護管理執行小組協調相關人員審議後，作為對當事人告知之依據。

5.7.3 本校個人資料檔案清冊中所列之個人資料檔案，除依法免為告知之個人資料檔案外，其對應之告知事項文件，應彙整集中供本校各單位查閱參考，並有版本識別與管理。

5.7.4 個人資料檔案之蒐集與處理

5.7.4.1 本校各單位以本校名義蒐集與處理特種個資時，應鑑別該特種個資之蒐集與處理符合以下其中之一條件，並將鑑別結果登載於個人資料檔案清冊中：

1. 法律明文規定。
2. 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
3. 當事人自行公開或其他已合法公開之個人資料。
4. 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
5. 為協助公務機關執行法定職務或非公務機關履行法定義

務必要範圍內，且事前或事後有適當安全維護措施。

6. 經當事人書面同意。

5.7.4.2 本校各單位以本校名義蒐集與處理特種個資以外個人資料檔案時，應鑑別該個人資料檔案之蒐集與處理符合以下條件之其中一項，並將鑑別結果登載於個人資料檔案清冊中：

1. 法律明文規定
2. 與當事人有契約或類似契約之關係且已採取適當之安全措施
3. 當事人自行公開或其他已合法公開之個人資料
4. 統計或學術研究且無從識別特定之當事人
5. 經當事人同意
6. 為增進公共利益所必要
7. 個人資料取自於一般可得之來源
8. 對當事人權益無侵害

5.7.5 個人資料檔案之利用

5.7.5.1 本校各單位應於個人資料檔案對應之告知事項所列之特定目的範圍內，對該個人資料檔案進行利用。

5.7.5.2 特種個資雖經當事人同意，但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用。

5.7.5.3　本校各單位利用個人資料為宣傳、推廣或行銷時，應明確告知當事人本校名稱及個人資料來源。首次利用個人資料為宣傳、推廣或行銷時，應提供當事人表示拒絕接受宣傳、推廣或行銷之方式，並支付所需費用；當事人表示拒絕宣傳、推廣或行銷後，應立即停止利用其個人資料宣傳、推廣或行銷。

5.7.6 受委託蒐集、處理與利用個人資料檔案

5.7.6.1　本校各單位受其他機關委託蒐集、處理與利用個人資料檔案前，應以該機關名義與該委託機關提供之告知事項，對當事人進行告知。並依照該告知事項於受委託範圍內，對該個人資料檔案進行蒐集、處理與利用。

5.7.7 國際傳輸

5.7.7.1　本校各單位以本校名義對個人資料檔案進行國際傳輸時，應確認個人資料檔案之接收地與利用目的包含於所傳輸之個人資料檔案對應之告知事項中，且接收地對於個人資料之保護有完善之法規，不致有損當事人權益之虞，方可以本校名義進行國際傳輸，如不符上述條件，仍需對個人資料檔案進行國際傳輸，應取得當事人書面同意，並以當事人名義進行個人資料檔案傳輸。

5.7.8 有關個人資料蒐集、處理及利用之作業管制詳細規定，另訂「個人資料蒐集、處理及利用管理程序書」規範之。

5.8 資料與設備安全管理

5.8.1 本校蒐集、處理與利用個人資料檔案之各單位，應確保個人資料檔案資料之輸入、處理、輸出、使用、保存、傳輸與銷毀之資料生命週期，皆有適切之控管，並對個人資料檔案相關設備應有實體安全防護與存取控制，以防止個人資料檔案遭竊取、竄改、毀損、滅失或洩漏。

5.8.2 本校各單位所屬人員透過網路對外傳輸個人資料檔案時，應對檔案或傳輸過程採用適當之加密機制，透過網路對內傳輸個人資料檔案時，應確認個人資料檔案有設定開啟密碼或開啟須經個人資料檔案身分認證。

5.8.3 本校各單位所屬人員除本校核可之雲端服務外，未經授權不得將個人資料檔案存放於外部儲存空間。

5.8.4 本校各單位所屬人員使用行動儲存裝置進行個人資料檔案之備份與暫存時，應確保儲存於行動儲存裝置之個人資料檔案經加密、編碼或設定開啟密碼等措施之保護，並妥善保管含有個人資料檔案之行動儲存裝置，防止遭遺失或竊取。

5.8.5 本校各單位所屬人員對於個人資料之存取應與本身業務範圍相關，任何人未經授權不得存取與個人業務無關之個人資料。

5.8.6 本校各單位公務文書及紙本郵件應有專人負責收發。

5.8.7 本校各單位所屬人員針對存有個人資料之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖。

5.8.8 本校各單位所涉及個人資料檔案之蒐集、處理與利用之伺服器、個人電腦及筆記型電腦應設定螢幕保護程式，並設定密碼或採取登出鎖定方式保護。

5.8.9 本校各單位所保有之個人資料檔案應建立保存期限，並確實辦理保存與銷毀。

5.8.10 有關文件、紀錄、相關電子檔之使用、保存、傳輸與銷毀及儲存媒體控管原則及方式，請參閱資訊安全管理制度(ISMS)「資訊資產管理程序書」。

5.8.11 有關實體資產，包括：軟體、硬體、環境等之控管原則及方式，請參閱資訊安全管理制度(ISMS)「實體安全管理程序書」。

5.8.12 有關辦公環境實體安全防護與螢幕保護程式設定等，請參閱資訊安全管理制度(ISMS)「辦公區域管理作業規範」。

5.9 人員安全管理

5.9.1 本校各單位所屬人員與委外人員皆應遵守「資訊安全政策」與「個人資料保護管理政策」及相關程序書與作業規範。

5.9.2 本校各單位所屬人員於服務期間皆應遵守「人員資訊安全守則」，於

業務上所獲知之機密資訊，非經主管授權不得對外透露。

5.9.3 本校各單位所屬人員於到職時應簽署「保密切結書」，並克盡保密之責。

5.9.4 本校各單位主管應依據業務作業所需之最小權限與最小資料範圍原則，授權並定期審查所屬人員對於個人資料檔案之存取權限與資料範圍，以確保本校各單位所屬人員對於個人資料檔案存取之必要性與適切性。

5.9.5 本校各單位應確保所屬人員離職時及時取消其識別碼，並應要求將執行業務所持有之個人資料（包括紙本及儲存媒介物）辦理交接。

5.9.6 針對員工違反資訊安全政策及程序者，應依正式懲戒程序處置相關違紀人員。

5.9.7 有關存取權限授權與審查之實施方式，請參閱資訊安全管理制度(ISMS)「存取控制管理程序書」。

5.9.8 有關簽署保密切結與違反資訊安全懲處之實施方式，請參閱資訊安全管理制度(ISMS)「人員安全與教育訓練程序書」與本校「職員工獎懲辦法」。

5.10 委外管理

5.10.1 本校各單位委託他人蒐集、處理或利用個人資料之全部或一部時，

應對受託者為適當之監督，並明確約定相關監督事項及方式。包括：

1. 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
2. 受託者採取之安全維護措施。
3. 有複委託者，其約定之受託者。
4. 受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。
5. 委託機關如對受託者有保留指示者，其保留指示之事項。
6. 委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。
7. 配合委託者為確認受託者執行之狀況所執行之查核，提供必要之資料與協助。

本校各單位應定期確認受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料，以及上述其他事項執行情況，並記錄確認結果。

5.10.2 有關對於受委託之監督管理實施方式，請參閱資訊安全管理制度(ISMS)「委外管理程序書」。

5.11 認知宣導及教育訓練

5.11.1 本校個人資料保護管理執行小組應規劃定期或不定期對本校各單位所屬人員教育訓練或認知宣導，本校各單位所屬人員應參加上述教育訓練或認知宣導，以明瞭個人資料保護相關法令規定、責任範圍、作業程序及應遵守之相關措施。.

5.11.2 有關個人資料保護教育訓練或認知宣導之實施方式,請參閱資訊安全管理制度(ISMS)「人員安全與教育訓練程序書」。

5.12 個人資料保護管理目標與績效評估

5.12.1 本校之個人資料保護管理整體目標，應延伸為各項展開目標，並有對應之績效監測、衡量、分析與評估，以確保達成個人資料保護管理整體目標。

5.12.2 有關個人資料保護管理目標與績效評估之實施方式，另訂「目標與績效管理程序書」規範之。

5.13 個人資料安全稽核機制

5.13.1 本校應訂定個人資料檔案安全稽核機制,定期或不定期檢查安全維護計畫所定相關事項是否落實執行。

5.13.2 有關個人資料檔案安全稽核機制之實施方式，請參閱「管理制度稽核作業程序書」。

5.14 個人資料使用紀錄、軌跡資料及證據保存

5.14.1 本校執行安全維護計畫各項程序及措施，應保存下列紀錄：

1. 個人資料之交付及傳輸。
2. 個人資料之維護、修正、刪除、銷毀及轉移。
3. 提供當事人行使之權利。
4. 存取個人資料系統之紀錄。
5. 備份及還原之測試。
6. 所屬人員權限之異動。
7. 所屬人員違反權限之行為。
8. 因應事故發生所採取之措施。
9. 定期檢查處理個人資料之資訊系統。
10. 教育訓練。
11. 安全維護計畫稽核及改善措施之執行。
12. 業務終止後處理紀錄

5.14.2 有關個人資料檔案安全維護計畫實施各項程序及措施紀錄管理之細部規定，請參閱「管理制度文件管理程序書」。

5.15 個人資料安全維護之整體持續改善

5.15.1 本校各單位於個人資料安全維護推行過程，應接受稽核，並針對稽核發現之缺失檢討其根本原因，提出消除已知缺失事項之改正措施與消除其根本原因防止再發之矯正措施。

5.15.2 有關改正措施與矯正措施之實施與追蹤方式，請參閱「矯正及預防

管理程序書」。

5.16 業務終止資料處理方法

5.16.1 本校業務終止後，其保有之個人資料之處理方式及留存紀錄如下：

1. 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。
2. 移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。
3. 刪除、停止處理或利用個人資料:刪除、停止處理或利用之方法、時間或地點。

5.16.2 有關本校業務終止資料處理之實施方式，另訂「業務終止後個人資料處理程序書」規範之。