高雄醫學大學

個人資料保護管理政策

機密等級：一般

文件編號：**PIMS-A-001**

版　　次：**1.1**

發行日期：**109/07/01**

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	108/01/29		謝志昌	初版
1.1	109/07/01	3~4、6~8	謝志昌	2.1 修訂個人資料保護管理制度(Personal Information Management System，以下簡稱 PIMS) 6.3 更新單位名稱 8 修訂文字

高雄醫學大學(以下簡稱本校)為落實個人資料之保護及管理並符合「個人資料保護法」與「個人資料保護法施行細則」、「私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法」之要求，特訂定個人資料保護管理政策(以下簡稱本政策)。本校個人資料保護管理之目標如下：

一、遵循個人資料相關法律法規要求。

二、正當、合法及透明之蒐集、處理與利用個人資料。

三、保障個人資料當事人權益。

四、維護個人資料安全防止竊取、竄改、毀損、滅失或洩漏。

1 個人資料之蒐集與處理

本校因營運所需取得或蒐集之包括但不限於個人之姓名、出生年月日、國民身分證統一編號(護照號碼)、特徵、指紋、婚姻、家庭、教育、職業等個人資料，應遵循我國個人資料保護法(以下簡稱個資法)等法令，不過度且符合目的、相關且適當並公平與合法地從事個人資料之蒐集與處理。而有需要經當事人同意之事實應負舉證責任。

2 個人資料之利用

2.1 本校所蒐集、處理之個人資料，應遵循我國個資法及本校個人資料保護管理制度(Personal Information Management System，以下簡稱

PIMS）之規範，且個人資料之使用為本校營運或業務所需，方可為本校承辦同仁利用。

2.2 本校於利用個人資料時，除需依個資法之特定目的必要範圍內為之外，如需為特定目的以外之利用時，將依據個資法第 20 條之規定辦理；倘有需取得當事人同意之必要者，本校應依法取得當事人之同意。

3 個人資料之國際傳輸

本校取得之個人資料，如有進行國際傳輸之必要者，應遵守個資法對於國際傳輸之規定包括不違反國家重大利益、不以迂迴方法向第三國傳遞或利用個人資料規避個資法等辦理，如國際條約或協定有特別規定、或資料接受國對於個人資料之保護未有完善之法令致有損害當事人權益之虞者，本校將不進行國際傳輸，以維護個人資料之安全。

4 個人資料之當事人權利行使

當本校接獲個人資料調閱或異動之需求時，應依個資法及本校所訂之程序，於合法範圍內進行當事人之個人資料查詢或請求閱覽、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。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

供申請方式之說明。

5 個人資料之目的外利用

5.1 本校因業務上所擁有之個人資料負有保密義務，除當事人之要求查閱，遇有公務機關要求提供當事人個人資料之情形，應請該公務機關釋明其要求提供個人資料行為，於個人資料保護法之依據，如所要求提供者為有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，本校提供個人資料前，亦須確認是否有個資法第六條第一項所適用之規定。

5.2 本校對個人資料之利用，除個資法第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

5.2.1 法律明文規定。

5.2.2 為增進公共利益所必要。

5.2.3 為免除當事人之生命、身體、自由或財產上之危險。

5.2.4 為防止他人權益之重大危害。

5.2.5 公務機關或學術研究機構基於公共利益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。

5.2.6 經當事人同意。

5.2.7 有利於當事人權益。

6 個人資料之保護

6.1 本校已成立個人資料保護組織，明確定義相關人員之責任與義務。

6.2 本校已建立與實施 PIMS ，以確認本政策之實行；全體員工及委外廠商應遵循 PIMS 之規範與要求，並定期審查 PIMS 之運作。

6.3 為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本校於資訊安全委員會下設置個人資料保護管理執行小組，負責 PIMS 之推行。並由教務處、學生事務處、總務處、產學營運處、國際事務處、秘書處、人力資源室、會計室、圖書資訊處、及相關教學單位推派人員組成。

6.4 個人資料檔案應建立管理制度，分級分類管理，並針對個人資料檔案蒐集、處理與利用過程建立安全管理規範。

6.5 為確保所有個人資料安全，應強化個人資料檔案資訊系統之存取安全，防止非法授權存取，維護個人資料之隱私性，應建立安全保護機制，並定期查核確認安全保護機制有效性。

6.6 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身分之登入通行碼，並視業務及重要性，考量其他輔助安全措施。

6.7 個人資料輸入、輸出、存取、更新、銷毀或分享等處理行為，應釐定使用範圍及調閱或存取權限。

6.8 本校各單位如遇有個人資料檔案發生竊取、竄改、毀損、滅失或洩漏等安全事件，應進行緊急因應措施，並依本校【個人資料安全事件管理程序書】通報程序辦理。

6.9 本校係以嚴密之措施、政策保護當事人之個人資料，包括本校之所有教職員工生，均受有完整之個資法及隱私權保護之教育訓練。倘有洩露個資之情事者，將依法追究其民事、刑事及行政責任。

6.10 本校之委外廠商或合作廠商與本校業務合作時，均應簽訂保密契約，使其充分瞭解個人資料保護之重要性及洩露個資之法律責任。倘有違反保密義務之情事者，將依法追究其民事及刑事責任。本校業務承辦單位，對於委外廠商或合作廠商有監督之職責，應於提供服務或合作過程，要求委外廠商或合作廠商符合本校之 PIMS 規定。

7 管理審查

7.1 本校個人資料保護及管理決議事項應納入資訊安全委員會報告，為確保本校矯正預防措施之有效運作，應落實管理審查機制，本校每年至少舉行一次資訊安全委員會議，並確實討論下列議題：

7.1.1 前次管理審查決議後續追蹤事項。

7.1.2 風險評鑑與風險管理結果。

7.1.3 內外部稽核結果。

7.1.4 關注方之意見或建議。

7.1.5 個人資料申訴抱怨事件。

7.1.6 已發生之個資事故。

7.1.7 改善個資保護之方法、技術與產品。

7.1.8 控制措施持續改進之有效性評量。

8 個人資料保護管理政策之修正權

本校之個人資料保護管理政策，每年定期或因時勢變遷或法令修正等事由，予以適當修訂，經「資訊安全委員會」決議後實施，修訂時亦同。