



中山醫學大學

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：4.1

發行日期：108.12.18

個人資料保護管理政策					
文件編號	PIMS-A-001	機密等級	一般	版次	4.1

目錄

壹、個人資料之蒐集與處理	1
貳、個人資料之利用及國際傳遞	1
參、個人資料之調閱與異動	2
肆、個人資料之例外應用	2
伍、個人資料之保護	2
陸、利害關係人之參與及期許	3
柒、個人資料保護政策之修正權	4

個人資料保護管理政策					
文件編號	PIMS-A-001	機密等級	一般	版次	4.1

中山醫學大學（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」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、依「個人資料保護法」、「個人資料保護法施行細則」與「教育體系資通安全暨個人資料管理規範」要求，保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀之過程。
- 二、為保護本校業務相關個人資料之安全，免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。
- 三、提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。
- 四、為提升同仁個人資料保護安全意識，每年定期辦理個人資料保護宣導教育訓練。
- 五、定期針對個人資料流程進行風險評鑑，鑑別可承受風險等級。

壹、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、透明且適當並公平與合法地從事個人資料之蒐集與處理，保持個人資料的正確性。而有需要經當事人同意之事實應負舉證責任。

貳、個人資料之利用及國際傳遞

- 一、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，將依據個資法第十六條之規定辦理；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。
- 二、本校所蒐集、處理之個人資料，應遵循我國個資法及本校個資管理制度之規範，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。
- 三、本校取得之個人資料，如有進行國際傳遞之必要者，定謹遵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之規定等原則辦理，又，倘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遞，以維護個人資料之安全。

個人資料保護管理政策					
文件編號	PIMS-A-001	機密等級	一般	版次	4.1

四、對歐盟其他國家的自然人提供貨物或服務，應在適當時，提出應對監管機構的策略。

參、個人資料之調閱與異動

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。

肆、個人資料之例外應用

一、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或有下列情形外，應符合個資法第十六條及相關法令規定，並以正式公文查詢外，本校不得對第三人揭露：

- (一)司法機關、監察機關或警政機關因偵查犯罪或調查證據所需者。
- (二)其他政府機關因執行公權力並有正當理由所需者。
- (三)與公眾生命安全有關之機關（構）為緊急救助所需者。

二、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：

- (一)法律明文規定。
- (二)為維護國家安全或增進公共利益所必要。
- (三)為免除當事人之生命、身體、自由或財產上之危險。
- (四)為防止他人權益之重大危害。
- (五)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。
- (六)有利於當事人權益。
- (七)經當事人同意。

伍、個人資料之保護

一、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。

個人資料保護管理政策					
文件編號	PIMS-A-001	機密等級	一般	版次	4.1

- 二、本校已建立與實施個人資料管理制度(PIMS)，以確認本政策之實行；全體員工及委外廠商應遵循個人資料管理制度（PIMS）之規範與要求，並定期審查 PIMS 之運作。
- 三、為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本校設置「中山醫學大學資訊安全暨個人資料保護委員會」，負責制定政策、監督及稽核個人資料保護管理機制之運作、評估及改善個資風險及應變處理緊急事件。
- 四、個人資料檔案應建立管理制度，分級分類管理，維護單位處理的個人資料分類清冊，並針對接觸人員建立安全管理規範。
- 五、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。
- 六、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。
- 七、個人資料輸入、輸出、存取、更新、銷毀或分享等處理行為，應維護處理紀錄，並釐定使用範圍及調閱或存取權限。
- 八、確保處理直接由未成年人蒐集的資訊受到特別保護。
- 九、本校各單位如遇有個人資料檔案發生遭人惡意破壞、毀損或作業不慎等安全事件，應進行緊急因應措施，並依本校【個人資料保護緊急應變處理作業說明書】通報程序辦理。
- 十、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。
- 十一、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。

陸、利害關係人之參與及期許

本校個人資料保護及管理決議事項應納入個人資料保護推動執行小組管理審查會報告，涉及重大決議之會議紀錄應提報主管機關（教育部）及利害關係人(如企業雇主、畢業校友、學生家長、本校教職員工生及其他與本校相關人士等)，如有任何回饋事項，將列入下次管理審查會議之討論議題。

個人資料保護管理政策					
文件編號	PIMS-A-001	機密等級	一般	版次	4.1

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管理審查會議，並確實討論下列議題：

- 一、過往管理審查之議案的處理狀態。
- 二、來自 PIMS 使用者之回饋。
- 三、由組織人員所辨識及提升之風險。
- 四、內外部稽核結果。
- 五、程序審查及紀錄。
- 六、資訊技術提升及替換之結果。
- 七、來自主管機關評估後之正式要求。
- 八、抱怨事件的處理。
- 九、已發生之資安事故及資料外洩事件。
- 十、管理目標與指標量測結果。

柒、個人資料保護政策實施與修正

- 一、本校之個人資料保護政策，每年定期或法令修正等事由，經「中山醫學大學資訊安全暨個人資料保護委員會」審核修訂後實施。
- 二、本政策應以書面、電子(E-MAIL、網頁公告)或其他方式傳達本校關注方共同遵守。