

文件編號	CMU-PIMS-D-021	機密等級	內部使用	版次	1.2
------	----------------	------	------	----	-----

流水號：



中國醫藥大學

CHINA MEDICAL UNIVERSITY

委外處理個人資料保護管理制度檢核表

填表日期： 年 月 日

委任單位						承辦人姓名				
受任人(廠商)名稱		聯絡人				電話				
編號	檢核項目	符合	部分符合	未符合	不適用	勾選「部分符合」、「未符合」「不適用」者，請於本欄填寫原因				
人員管理										
1	處理個資是否採取權限區隔，非專責處理特定個資者不得具有存取或查閱個資之權限？									
2	是否已具備利用事務機器(例影印機、印表機或傳真機)列印、傳真或使用個資後，應立即取走之安全觀念？									
3	處理個資檔案之人員職務異動時，是否列冊移交相關儲存媒體及資料？									
4	處理個資檔案之人員職務異動時，接替人員是否於相關系統重置通行碼，並視需要更換使用者識別帳號？									
5	處理個資檔案之外部人員，是否簽訂保密切結書相關文件？									
6	處理個資檔案之人員離職或合約終止時，是否取消或停用其使用者識別帳號？									
作業管理										
7	受任人(廠商)是否遵守個人資料保護法的相關規定？									
8	受任人(廠商)是否依本校個人資料保護管理制度簽訂「委外廠商保密切結書」？									
9	受任人(廠商)是否依本校所列的或其所指示範圍內蒐集、處理、利用個資？									
10	受任人(廠商)是否有複委託者？									
11	交換紙本個資時，是否採取彌封或其他具備保密機制之傳遞方式？									
12	交換個資檔案時，是否對資料檔案加密，或是透過加密通道、機制傳送？									
13	個資檔案處理完畢，是否定期進行銷毀或刪除？									
14	儲存個資檔案之電腦或相關設備如需報廢或移轉他用，是否刪除其內所儲存之個資檔案？									
15	委外建檔的個資檔案，是否於委外合約中載明所處理之個資保密義務、資訊安全相關責任及違反之罰則？									
物理環境管理										
16	是否依據各業務屬性，指定人員負責管理儲存個資檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息？									
17	儲存個資之資訊設備是否置放於實體安全的環境(如：具門禁控管、監視設備之辦公區域或機房)？									

文件編號	CMU-PIMS-D-021	機密等級	內部使用	版次	1.2
18	儲存個資檔案紙本或可攜式設備(例 USB、磁碟)等相關儲存媒體，是否置於實體保護之環境？(例具門禁控管、監視設備之辦公區域、上鎖的櫃子)				
19	儲存個資檔案之媒體是否有攜出、拷貝或複製的管控機制？				
技術管理					
20	處理個資檔案之個人電腦，是否設置使用者帳號及通行碼？				
21	是否將存放敏感性個資的電腦與外部網路隔絕(如：防火牆)？				
22	處理個資檔案之個人電腦是否安裝防毒程式並維持最新的病毒碼？				
23	處理個資檔案之個人電腦是否安使用尚支援Windows Update的作業系統？				
認知					
24	處理個資檔案之受任人(廠商)是否曾接受個人資料保護相關教育訓練？				
紀錄機制					
25	交換個資時，是否記錄轉交或傳輸行為之流向？				
26	受任人(廠商)是否有設計個資蒐集目的消失或屆滿之資料刪除程序？				
27	是否針對先前查檢不符合事項進行提出討論並找出原因？				
28	是否針對先前查檢不符合事項進行改善？				
廠商 公司章		負責人 簽章			
複檢結果 (以下欄位由中國醫藥大學複檢時填寫)					
檢查項目					
檢查結果		檢查結果 <input type="checkbox"/> 符合 <input type="checkbox"/> 不符本校要求 不符內容：			
檢查日期		檢查人 簽章		權責主管 簽章	