

臺北市通訊診療實施計畫資訊安全自我檢核表

檢核單位名稱：_____

檢核日期：_____

檢核人員：_____

	診所及醫院 檢核項目	檢核結果	備註	資料 提供人 簽名欄
1.	醫療作業所需使用之硬體設備(電腦、伺服器、筆電)或操作平台是否有區隔並為專屬使用？	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明。	
2.	落實醫療/醫務作業系統平台所使用之硬體設備之控管(電腦/筆電)，且於該列管之設備僅得以執行醫療作業相關之事務(包含電子郵件)。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明或提供列管設備之清冊。	
3.	醫務/醫療作業使用之電腦、筆電或伺服器皆已完成安裝防毒軟體。請檢視防毒軟體之病毒碼是否已更新至最新版本。 建議避免使用網路上提供之免費使用防毒軟體以降低風險。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請提供防毒軟體名稱與病毒碼最新一次更新日期截圖作為佐證。	
4.	確認最近一次作業系統安全性更新並將更新日期紀錄存查。每月更新一次為宜。 如設備使用之作業系統版本較老舊且品牌原廠不再提供版本更新服務(EOS, End of Service)，則須改採符合軟體更新時效之應用軟體，或進行存取權限控管、增加資安防護設備(如防火牆)以及密碼應符合高複雜度以確保整體資訊安全機制之運行。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請提供作業系統安全最新一次更新截圖作為佐證。	
5.	啟動螢幕保護並執行限制操作時間螢幕鎖定設定。建議螢幕鎖定之時間設定以不超過15分鐘為原則。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請提供截圖作為佐證。	
6.	電腦密碼是否有符合安全性設定？ 1. 最小密碼長度是否為8碼或以上； 2. 密碼必須符合複雜性需求是否為	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請提供控制台「本機安全性原則」截圖作為佐證。	

	診所及醫院 檢核項目	檢核結果	備註	資料 提供人 簽名欄
	開啟； 3. 密碼最長有效期是否為 90 天或以下，但如有密碼外洩之風險則應立即修改。			
7.	密碼應妥善保管避免外洩，不得將密碼張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明密碼保管機制。	
8.	執行醫療/醫務作業使用之電腦/筆電請啟動本機防火牆設定，可啟動設置阻擋可疑連線或白名單建立之功能設定。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請提供本機防火牆設定截圖作為佐證。	
9.	遠端連線軟體或手機應用程式(APP)需有安全加密通道(支援 TLS1.2 以上)及記錄(log)保存機制。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若有使用遠端連線軟體或手機應用程式(APP)，請說明是否支援安全加密通道(支援 TLS1.2 以上)及紀錄保存(log)機制。	
10.	如業務需要使用可攜式媒體儲存(USB、行動硬碟)傳遞含有機敏性個資或機密資料，須另採加密機制(如:zip 加密)保護本機資料。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明資料加密機制。	
11.	避免安裝或連結未經授權及來路不明之軟硬體。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請提供控制台「解除安裝與變更程式」截圖作為佐證。	
12.	啟用系統安全性設定之稽核原則設定。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請提供控制台「本機安全性原則」截圖作為佐證。	
13.	定期執行重要資料之備份作業並加密處理。建議備份資料採異機(指非本機儲存空間)存放。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明並提供佐證。	
14.	內部員工私接 MODEM、ADSL 及無線網路卡等網路通訊設備易造成病患個資外洩風險，對外連線須有適切的管制措施。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明網路通訊設備的管制措施。	
15.	醫療/醫務作業用電腦資產需造冊列管並設定專人保管並於安全場所存放，非授權作業人員不得操作使	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明作業用電腦資產存放與授權使用方式，並提供監視錄影影片存放 3 個月以上的佐	

	診所及醫院 檢核項目	檢核結果	備註	資料 提供人 簽名欄
	用。可對設備使用/保存場所進行適當的監視錄影，監視錄影之影片建議存檔3個月以上。		證截圖。	
16.	任何儲存資訊之電子設備於報廢/丟棄之前，應將儲存資訊刪除，並徹底消磁或銷毀至無法解讀之程度。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明儲存資訊之電子設備的報廢/丟棄處理程序。	
17.	執行醫療作業是否使用屬於大陸廠牌資通訊產品(含硬體、軟體及服務)有資安疑慮產品？	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若有使用大陸廠牌資通訊硬體，請說明品牌:_____ 若有使用大陸廠牌資通訊軟體，請說明品牌:_____ 若有使用大陸廠牌資通訊服務，請說明品牌:_____ (建議不使用具資通安全疑慮的產品，例如 ZOOM、杭州海康威視數位技術股份有限公司(Hikvision)、普聯技術有限公司(TP-Link)、華為技術有限公司(Huawei)、浙江大華技術股份有限公司(Dahua)、「廣東歐加控股有限公司/廣東行動通訊有限公司(OPPO)」、「小米集團(MI)(含紅米)」、「浙江大華技術股份有限公司(Dahua)」、「TOTOLINK」、荷蘭商聯想、法國 Alcatel-Lucent 及美國 Fortinet 等)	
18.	執行醫療作業前，相關人員是否簽署保密切結書，以達到個資保護之目的？	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明執行方式或提供佐證資料。	
19.	執行醫療作業前，被診療對象是否簽署個人資料保護同意書，以達到個資保護之目的？	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明執行方式或提供佐證資料。	
20.	通訊診療過程，醫師應於醫療機構內實施，並確保病人之隱私。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明。	
21.	醫療/醫務作業系統平台所使用之帳號應禁止共用，並定期辦理清查作業。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明。	
22.	應視醫療/醫務作業系統平台特性限定其作業時間，以減少未經授權人員存取系統之機會。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明。	

診所及醫院 檢核項目		檢核結果	備註	資料 提供人 簽名欄
23.	醫療/醫務作業系統平台須有相關 log 紀錄系統使用情形（包括使用者帳號、來源 IP、登入日期等）。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	若符合，請說明。	
24.	若實施電子病歷管理作業，應有符合「醫療機構電子病歷製作及管理辦法」之管理措施。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	若符合，請提供相關管理措施說明。	

	醫院 檢核項目	檢核結果	備註	資料 提供人 簽名欄
25.	<p>確認最近一次應用系統與資料庫系統安全性更新並維持最新狀態，落實系統更新日期紀錄存查。</p> <p>(如設備使用之應用系統與資料庫系統版本較老舊且品牌原廠不再提供版本更新服務(EOS, End of Service)，則須改採符合軟體更新時效之應用軟體，或進行存取權限控管、增加資安防護設備(如防火牆)以及密碼應符合高複雜度以確保安全性。</p>	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	若符合，請說明。	
26.	<p>密碼安全性原則建議如下：</p> <p>密碼輸入錯誤超過五次則帳號鎖定15分鐘。</p>	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	若符合，請提供控制台「本機安全性原則」截圖作為佐證。	
27.	<p>建立共用資料夾(如:網路芳鄰)存取限制。</p>	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	若符合，請說明。	
28.	<p>是否依網路服務需要區隔獨立的邏輯網域，並建立適當之防護措施，以管制過濾網域間之資料存取？</p>	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	若符合，請說明。	
29.	<p>如有遠端存取維護情形，針對透過遠端執行特定之功能及存取相關資訊是否採加密機制，以保護遠端存取連線之機密性？</p>	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	若符合，請說明遠端存取維護如何保護連線內容之機密性。	
30.	<p>是否針對外部連接之資訊交換，建立適當之交換程序及安全保護措施，以確保資訊之完整性及機密性(如採行識別碼通行碼管制、電子資料加密或電子簽章認證等)？是否針</p>	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	若符合，請說明安全保護措施及監控記錄的保存方式。	

	醫院 檢核項目	檢核結果	備註	資料 提供人 簽名欄
	對重要資料的交換過程，保存適當之監控紀錄？			
31.	所有銷毀/報廢的電子設備應留存紀錄(設備名稱/型號、銷毀日期、處理人員、照片..等)，以備日後查詢。	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	若符合，請說明執行方式或提供佐證資料。	

*以上檢核項目參考衛生福利部「基層醫療院所資安防護參考指引」，請院所每年定期進行檢核並持續進行改善。

*依「醫療法」第12條，醫療機構設有病房收治病者為醫院，僅應門診者為診所。

附件、佐證資料

檢核項目	佐證資料
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	

檢核項目	佐證資料
28	
29	
30	
31	