醫療器材網路安全之業者揭露聲明書（Manufacturer's Disclosure Statement for Medical Device Security ）

項次	細項次	主類別	項目編號	要求項目問題	符合 Yes	不符合 No	不適用 N/A	簡述符合、不符合或不適用之原因	紀錄文件
1		**DOC-產品基本資料**							
1.1	1	DOC-產品基本資料	DOC-1	製造商名稱	v			ABC公司	
1.2	2	DOC-產品基本資料	DOC-2	設備描述	v			葡萄糖試驗系統	
1.3	3	DOC-產品基本資料	DOC-3	設備型號	v			ABC-01	
1.4	4	DOC-產品基本資料	DOC-4	文件編號	v			MDS2-01	
1.5	5	DOC-產品基本資料	DOC-5	製造商聯絡資訊	v			sales@ABCcompany.com	
1.6	6	DOC-產品基本資料	DOC-6	設備在連網環境中的預期用途	v			應用程式須配合ABC血糖試紙設計為與ABC血糖機使用，適用於定量檢測採自指尖、手掌、前臂和上臂的新鮮微血管全血的血糖，可幫助有效進行血糖監控。 ABC血糖試紙與ABC血糖機合用，適用於糖尿病患者的自我體外診斷檢測，同時透過藍芽將血糖資訊傳輸至ABC應用程式與管理軟體並上傳至ABC線上糖尿病管理系統，幫助專業醫護人員在臨床診療環境下的體外診斷檢測。	
1.7	7	DOC-產品基本資料	DOC-7	文件發布日期	v			2021-08-11	
1.8	8	DOC-產品基本資料	DOC-8	協同漏洞披露：製造商是否有針對此設備的漏洞披露程序？	v			上市後監督程序內包含此漏洞披露程序	
1.9	9	DOC-產品基本資料	DOC-9	ISAO：製造商為情資分享和分析(ISAC)組織的會員？		v			
1.10	10	DOC-產品基本資料	DOC-10	圖表：是否有可用的網路或資料流圖來說明與其他系統元件或預期外部資源的連接？	v			詳見資料流向圖DFD顯示	
1.11	11	DOC-產品基本資料	DOC-11	SaMD：軟體是否為醫療器材本體（即僅軟體，無硬體）？		v			
	12	DOC-產品基本資料	DOC-11.1	SaMD 是否包含作業系統？			v		
	13	DOC-產品基本資料	DOC-11.2	SaMD 是否依賴擁有者/運營商提供的作業系統？			v		
	14	DOC-產品基本資料	DOC-11.3	SaMD 是否由製造商託管？			v		
	15	DOC-產品基本資料	DOC-11.4	SaMD 是否由客戶託管？			v		
2		**MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)**							
2.1	16	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-1	此設備能否顯示、傳輸、儲存或修改使用者可識別資訊（例如受保護的電子化醫療健康資訊 (ePHI)）？	v				
2.2	17	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-2	設備是否保留使用者身分資訊？	v			保存在雲端資料庫及手機APP中	
	18	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-2.1	設備是否將使用者身分資訊臨時保存在揮發性儲存設備中（即，直到通過斷電或重置清除）		v			
	19	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-2.2	設備是否將使用者身分資訊永久儲存在內部媒體上？	v			保存於手機APP中	
	20	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-2.3	使用者身分資訊是否保存在設備的非揮發性儲存設備中，直到明確刪除？	v				
	21	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-2.4	設備是否將使用者身分資訊儲存在資料庫中？	v				
	22	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-2.5	設備是否允許設定在儲存到長期解決方案後自動刪除本地使用者身分資訊？		v			
	23	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-2.6	設備是否與其他系統輸入/輸出使用者身分資訊（例如，穿戴式監控設備可能會將使用者身分資訊輸出至伺服器）？	v				
	24	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-2.7	設備在斷電或電力服務中斷期間是否保留使用者身分資訊？	v				
	25	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-2.8	設備是否允許服務技術人員移除內部資料（例如，單獨銷毀或客戶保留）？	v			可移除APP，則歷史資料消失	

	26	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-2.9	設備是否允許將使用者身分資訊記錄儲存在與設備作業系統不同的位置（即輔助內部儲存、備用儲存分割或遠端儲存位置）？		v			
2.3	27	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3	設備是否具有用於傳輸、輸入/輸出使用者身分資訊的機制？	v				
	28	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3.1	設備是否顯示使用者身分資訊（例如影片顯示等）？		v			
	29	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3.2	設備是否產生包含使用者身分資訊的拷貝報告或圖像？		v			
	30	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3.3	設備是否從可移除式媒體（例如，可攜式硬碟、USB 硬碟、DVD-R/RW、CD-R/RW、磁帶、CF/SD 卡、記憶卡等）中搜尋使用者身分資訊或將使用者身分資訊記錄到其中？）？		v			
	31	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3.4	設備是否通過專用電纜連接（例如 RS-232、RS-423、USB、FireWire 等）傳輸/接收或輸入/輸出使用者身分資訊？	v				
	32	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3.5	設備是否通過有線網路連接（例如 RJ45、光纖等）傳輸/接收使用者身分資訊？		v			
	33	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3.6	設備是否通過無線網路連接（例如 WiFi、藍牙、NFC、紅外線、蜂巢式網路等）傳輸/接收使用者身分資訊？		v			
	34	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3.7	設備是否通過外部網路（例如 Internet）傳輸/接收使用者身分資訊？		v			
	35	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3.8	設備是否通過掃描檔案輸入使用者身分資訊？		v			
	36	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3.9	設備是否通過專用協定傳輸/接收使用者身分資訊？	v				
	37	MPII-使用者身分資訊的管理(MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION, MPII)	MPII-3.10	設備是否使用任何其他機制來傳輸、輸入或輸出使用者身分資訊？		v			
3		**ALOF-自動登出 (AUTOMATIC LOGOFF, ALOF)：如果設備閒置一段時間，設備能夠防止未經授權的使用者存取和濫用**							
3.1	38	ALOF-自動登出 (AUTOMATIC LOGOFF, ALOF)	ALOF-1	設備是否可以設定為在預定的不活動時間（例如，自動登出、會話鎖定、受密碼保護的螢幕保護程式）後強制重新驗證使用者登入？	v				
3.2	39	ALOF-自動登出 (AUTOMATIC LOGOFF, ALOF)	ALOF-2	自動登出/螢幕鎖定等時間長度，是否可以被使用者或管理員設定？		v		出廠前即設定完成，不可修改	
4		**AUDT-稽核控制(AUDIT CONTROLS, AUDT)：能夠可靠地審核設備上的活動**							
4.1	40	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-1	醫療器材能否在標準作業系統日誌之外建立額外的稽核日誌或報告？<Ex 誰登入、輸入那些查詢項目等等, 如果這題是No, 則1.1-3.1都是N/A>	v				
	41	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-1.1	稽核日誌是否記錄了使用者 ID？			v		

	42	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-1.2	稽核日誌中是否存在其他的使用者身份資訊？			v		
4.2	43	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2	是否有事件是否記錄在稽核日誌中？如果是，請指明稽核日誌中記錄了以下哪些事件：	v				
	44	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.1	成功的登入/登出嘗試？			v		
	45	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.2	登入/登出嘗試不成功？			v		
	46	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.3	修改系統帳號使用者權限？			v		
	47	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.4	建立/修改/刪除系統帳號使用者？			v		
	48	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.5	臨床或 PII 資料的呈現（例如顯示、影印）？			v		
	49	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.6	建立/修改/刪除資料？			v		
	50	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.7	從可移除式媒體（例如 USB 驅動程式、外部硬碟驅動程式、DVD）輸入/輸出資料？			v		
	51	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.8	通過網路或端點連接接收/傳輸資料或命令？			v		
	52	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.8.1	遠端或現場支援？			v		
	53	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.8.2	應用程序程式介面（API）和類似活動？			v		
	54	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.9	緊急存取？			v		
	55	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.10	其他事件（例如，軟體更新）？			v		
	56	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-2.11	是否更詳細地記錄了稽核能力？			v		
4.3	57	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-3	擁有者/使用者能否定義或選擇在稽核日誌中記錄哪些事件？	v				
4.4	58	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-4	在事件的稽核日誌中捕獲的資訊屬性列表是否可用？	v				
	59	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-4.1	稽核日誌是否記錄日期/時間？			v		
	60	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-4.1.1	日期和時間可以通過網路時間協定(NTP) 或等效時間源同步嗎？			v		
4.5	61	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-5	稽核日誌內容可以輸出嗎？	v				
	62	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-5.1	通過實體媒體？			v		
	63	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-5.2	通過 IHE 資料追蹤和節點鑑別 (ATNA) 設定文件到 SIEM嗎？			v		
	64	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-5.3	通過其他通訊（例如，外部服務設備、行動應用程序）？			v		
	65	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-5.4	稽核日誌是在傳輸過程中還是在儲存設備上加密？			v		
4.6	66	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-6	擁有者/使用者可以監控/審查稽核日誌嗎？	v				
4.7	67	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-7	稽核日誌是否受到修改保護？	v				
	68	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-7.1	稽核日誌是否受到存取保護？	v				
4.8	69	AUDT-稽核控制(AUDIT CONTROLS, AUDT)	AUDT-8	設備可以分析稽核日誌嗎？			v		
5		**AUTH-授權（AUTHORIZATION, AUTH）：設備決定使用者授權的能力**							
5.1	70	AUTH-授權 (AUTHORIZATION, AUTH)	AUTH-1	裝置是否通過系統帳號使用者登入要求或其他機制阻止未經授權的系統帳號使用者存取？	v				
	71	AUTH-授權 (AUTHORIZATION, AUTH)	AUTH-1.1	是否可以將設備設定為用使用者的聯合憑證管理進行授權（例如，LDAP、OAuth）？					
	72	AUTH-授權 (AUTHORIZATION, AUTH)	AUTH-1.2	客戶能否將群組原則擴展至設備（例如 Active Directory）？					
	73	AUTH-授權 (AUTHORIZATION, AUTH)	AUTH-1.3	是否需要任何特定的群組、組織單位或群組原則？					
5.2	74	AUTH-授權 (AUTHORIZATION, AUTH)	AUTH-2	是否可以根據“身分”（例如，一般帳號、管理員帳號和/或服務帳號(更新軟體用..資料庫服務用)等）為系統帳號使用者給予不同的權限等級？	v				

5.3	75	AUTH-授權 (AUTHORIZATION, AUTH)	AUTH-3	裝置擁有者/使用者能否授予自己不受限制的管理權限（例如，通過本地 root 或管理員帳戶存取作業系統或應用程式）？	v				
5.4	76	AUTH-授權 (AUTHORIZATION, AUTH)	AUTH-4	設備是否授權或控制所有 API 存取請求？	v				
5.5	77	AUTH-授權 (AUTHORIZATION, AUTH)	AUTH-5	預設情況下，設備是否以受限存取模式或"自訂主控台"運行？			v		
6		**CSUP-網路安全產品升級（CYBER SECURITY PRODUCT UPGRADES, CSUP）：現場服務人員、遠端服務人員或授權客戶人員安裝 /升級設備安全修補程式的能力**							
6.1	78	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-1	設備是否包含任何在其使用壽命期間可能需要安全更新的軟體或韌體，無論是來自設備製造商還是來自軟體/韌體的第三方廠商？如果否，請對本節中的問題回答"N/A"	v				
6.2	79	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-2	設備是否包含作業系統？如果是，請完成 CSUP-2.1 ~ CSUP-2.4	v			設備包含APP與硬體裝置	
	80	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-2.1	設備文件是否提供擁有者/使用者安裝修補程式或軟體更新的說明？	v				
	81	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-2.2	設備是否需要經銷商或經銷商授權的服務來安裝修補程式或軟體更新？		v			
	82	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-2.3	設備是否具有接收遠端安裝修補程式或軟體更新的能力？	v				
	83	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-2.4	醫療儀器製造商是否允許在未經製造商允許的情況下安裝任何第三方廠商（例如 Microsoft）的安全更新？	v			APP OS 可進行安全更新	
6.3	84	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-3	設備是否包含驅動程式和韌體？如果是，請完成 CSUP3.1 ~ CSUP3.4	v				
	85	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-3.1	設備文件是否提供擁有者/使用者安裝修補程式或軟體更新的說明？		v			
	86	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-3.2	設備是否需要經銷商或經銷商授權的服務來安裝修補程式或軟體更新？		v			
	87	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-3.3	設備是否具有接收遠端安裝修補程式或軟體更新的能力？	v				
	88	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-3.4	醫療儀器製造商是否允許在未經製造商允許的情況下安裝任何第三方廠商（例如 Microsoft）的安全更新？	v				
6.4	89	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-4	設備是否包含防毒軟體？如果是，請完成 CSUP4.1~ CSUP4.4			v		
	90	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-4.1	設備文件是否提供擁有者/使用者安裝修補程式或軟體更新的說明？			v		
	91	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-4.2	設備是否需要經銷商或經銷商授權的服務來安裝修補程式或軟體更新？			v		
	92	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-4.3	設備是否具有接收遠端安裝修補程式或軟體更新的能力？			v		
	93	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-4.4	醫療儀器製造商是否允許在未經製造商允許的情況下安裝任何第三方廠商（例如 Microsoft）的安全更新？			v		
6.5	94	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-5	設備是否包含非作業系統商業現成元件？如果是，請完成 CSUP5.1 ~ CSUP5.4			v		
	95	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-5.1	設備文件是否提供擁有者/使用者安裝修補程式或軟體更新的說明？			v		
	96	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-5.2	設備是否需要經銷商或經銷商授權的服務來安裝修補程式或軟體更新？			v		

	97	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-5.3	設備是否具有接收遠端安裝修補程式或軟體更新的能力？			v		
	98	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-5.4	醫療儀器製造商是否允許在未經製造商允許的情況下安裝任何第三方廠商（例如 Microsoft）的安全更新？			v		
6.6	99	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-6	設備是否包含其他軟體元件（例如，資產管理軟體、憑證管理）？如果是，請在註釋中提供詳細資訊或參考並完成 CSUP6.1 ~ CSUP6.4			v		
	100	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-6.1	設備文件是否提供擁有者/使用者安裝修補程式或軟體更新的說明？			v		
	101	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-6.2	設備是否需要經銷商或經銷商授權的服務來安裝修補程式或軟體更新？			v		
	102	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-6.3	設備是否具有接收遠端安裝修補程式或軟體更新的能力？			v		
	103	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-6.4	醫療儀器製造商是否允許在未經製造商允許的情況下安裝任何第三方廠商（例如 Microsoft）的安全更新？			v		
6.7	104	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-7	當更新被允許安裝時，製造商是否會通知客戶？	v				
6.8	105	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-8	設備是否執行軟體更新的自動安裝？		v			
6.9	106	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-9	製造商是否有可安裝在設備上的第三方軟體的允許名單？			v		
6.10	107	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-10	擁有者/使用者是否可以自己在設備上安裝製造商認可的第三方軟體嗎？			v		
	108	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-10.1	系統是否有機制可以防止安裝未經允許的軟體(非製造商認可的第三方軟體)？			v		
6.11	109	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-11	製造商是否制定評估設備漏洞和更新的流程？	v				
	110	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-11.1	製造商向客戶所提供的更新，是否是經過先行審查和認證通過？	v				
	111	CSUP-網路安全產品升級 (CYBER SECURITY PRODUCT UPGRADES, CSUP)	CSUP-11.2	是否有一個週期更新審查機制？	v				
7		**DIDT-醫療資料去識別化 (HEALTH DATA DE-IDENTIFICATION, DIDT)：設備直接刪除允許識別使用者的資訊的能力**							
7.1	112	DIDT-醫療資料去識別化 (HEALTH DATA DE-IDENTIFICATION, DIDT)	DIDT-1	該設備是否提供對使用者身分資訊進行去識別化的整合功能？		v			
	113	DIDT-醫療資料去識別化 (HEALTH DATA DE-IDENTIFICATION, DIDT)	DIDT-1.1	設備是否支援符合 DICOM 去識別化標準的去識別化設定文件？			v		
8		**DTBK-資料備份和災難恢復 (DATA BACKUP AND DISASTER RECOVERY, DTBK)：在設備資料、硬體、軟體或站點設定資訊損壞或破壞後恢復的能力**							
8.1	114	DTBK-資料備份和災難恢復 (DATA BACKUP AND DISASTER RECOVERY, DTBK)	DTBK-1	設備是否長期保存使用者身分資訊/病患資訊（例如 PACS）？	v				

8.2	115	DTBK-資料備份和災難恢復(DATA BACKUP AND DISASTER RECOVERY, DTBK)	DTBK-2	設備是否具有“恢復原廠設定”功能，可以恢復製造商提供的初始設備設定？	v				
8.3	116	DTBK-資料備份和災難恢復(DATA BACKUP AND DISASTER RECOVERY, DTBK)	DTBK-3	設備是否具有完整資料備份於可移除式媒體的功能？	v				
8.4	117	DTBK-資料備份和災難恢復(DATA BACKUP AND DISASTER RECOVERY, DTBK)	DTBK-4	設備是否具有完整資料備份於遠端儲存媒體的功能？	v				
8.5	118	DTBK-資料備份和災難恢復(DATA BACKUP AND DISASTER RECOVERY, DTBK)	DTBK-5	設備是否具備系統設定檔、修補程式修復、軟體修復等備份能力？	v				
8.6	119	DTBK-資料備份和災難恢復(DATA BACKUP AND DISASTER RECOVERY, DTBK)	DTBK-6	設備是否提供檢查備份完整性和驗證性的能力？	v				
9		**EMRG-緊急存取(EMERGENCY ACCESS, EMRG)：在需要立即存取的使用者身分資訊的醫療緊急情況下，設備使用者存取使用者身分資訊的能力**							
9.1	120	EMRG-緊急存取(EMERGENCY ACCESS, EMRG)	EMRG-1	設備是否包含緊急存取（即“破窗”）功能？			v		
10		**IGAU-醫療資料完整性和驗證性 (HEALTH DATA INTEGRITY AND AUTHENTICITY, IGAU)：設備如何確保設備上儲存的資料未被未經授權的來源端更改或破壞**							
10.1	121	IGAU-醫療資料的完整性和驗證性 (HEALTH DATA INTEGRITY AND AUTHENTICITY, IGAU)	IGAU-1	設備是否提供儲存醫療資料的資料完整性檢查機制（例如：雜湊函數或數位簽章）？	v				
10.2	122	IGAU-醫療資料的完整性和驗證性 (HEALTH DATA INTEGRITY AND AUTHENTICITY, IGAU)	IGAU-2	設備是否為儲存的醫療資料提供錯誤/故障 保護和還原機制？（例如 RAID-5）	v				
11		**MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)：設備有效預防、檢測和刪除惡意軟體（ malware）的能力**							
11.1	123	MLDP-惡意軟體檢測/保護(MALWARE DETECTION/PROTECTION, MLDP)	MLDP-1	裝置上是否具有運作可執行軟體的能力<Ex: windows OS 可以運作antivirus軟體，但arduino版不能>		v			
11.2	124	MLDP-惡意軟體檢測/保護(MALWARE DETECTION/PROTECTION, MLDP)	MLDP-2	設備是否支援使用防毒/惡意軟體（或其他防毒/惡意軟體機制）？若有，在備註中提供詳細資訊或參考		v			
	125	MLDP-惡意軟體檢測/保護(MALWARE DETECTION/PROTECTION, MLDP)	MLDP-2.1	設備是否預設包含防毒/惡意軟體？			v		
	126	MLDP-惡意軟體檢測/保護(MALWARE DETECTION/PROTECTION, MLDP)	MLDP-2.2	設備是否提供防/惡意毒軟體作為選項？			v		
	127	MLDP-惡意軟體檢測/保護(MALWARE DETECTION/PROTECTION, MLDP)	MLDP-2.3	設備文件是否允許擁有者/使用者安裝或更新防毒/惡意軟體？			v		

	128	MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)	MLDP-2.4	設備擁有者/使用者能否獨立（重新）設定防毒/惡意軟體設定？			v		
	129	MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)	MLDP-2.5	設備的使用者介面中是否會出現惡意軟體偵測通知？			v		
	130	MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)	MLDP-2.6	當偵測到惡意軟體時，只有製造商授權的人員才能修復系統嗎？			v		
	131	MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)	MLDP-2.7	惡意軟體偵測通知是否會被記錄成文件？			v		
	132	MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)	MLDP-2.8	防毒/惡意軟體是否有任何限制（例如，購買、安裝、設定、排程）？			v		
11.3	133	MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)	MLDP-3	如果 MLDP-2 的答案是否定的，並且無法在設備上安裝防毒軟體，是否有其他補償控制措施可以使用？	v			透過APP作業系統更新維護	
11.4	134	MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)	MLDP-4	設備是否採用應用程序白名單來限制允許在設備上運行的軟體和服務？	v				
11.5	135	MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)	MLDP-5	設備是否採用本機入侵偵測/預防系統？		v			
	136	MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)	MLDP-5.1	客戶是否可以自行設定本機入侵偵測/預防系統嗎？		v			
	137	MLDP-惡意軟體檢測/保護 (MALWARE DETECTION/PROTECTION, MLDP)	MLDP-5.2	客戶是否可以自行安裝本機入侵偵測/預防系統嗎？		v			
12		**NAUT-節點鑑別 (NODE AUTHENTICATION, NAUT)：設備鑑別資料夥伴/節點的能力**							
12.1	138	NAUT-節點鑑別 (NODE AUTHENTICATION, NAUT)	NAUT-1	設備是否提供/支援任何節點身分鑑別方法，以確保資料來源端和目地端互相知道並接收已授權的傳輸資訊（例如 Web API、SMTP、SNMP）？	v				
12.2	139	NAUT-節點鑑別 (NODE AUTHENTICATION, NAUT)	NAUT-2	是否支援網路存取控制機制（例如，設備是否有內部防火牆，或使用網路連接白名單）？	v			只開放特定連接埠	
	140	NAUT-節點鑑別 (NODE AUTHENTICATION, NAUT)	NAUT-2.1	防火牆規則集是否有被記錄並可供審查？		v			
12.3	141	NAUT-節點鑑別 (NODE AUTHENTICATION, NAUT)	NAUT-3	設備是否使用以憑證為基礎的網路連接身分鑑別？		v			
13		**CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)：在確定適當的安全控制時，必須考慮所有網路和可移除式媒體連接。本節列出設備中可能存在的連接功能**							
13.1	142	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1	設備是否具有硬體連接功能？		v			
	143	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1.1	設備是否支援無線連接？	v				
	144	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1.1.1	設備是否支援 Wi-Fi？		v			

	145	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1.1.2	設備是否支援藍牙？	v				
	146	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1.1.3	設備是否支援其他無線網路連接（例如 LTE、Zigbee）？		v			
	147	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1.1.4	設備是否支援其他無線連接（例如，自定義 RF 控制、無線探測器）？		v			
	148	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1.2	設備是否支援實體連接？		v			
	149	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1.2.1	設備是否有可用的 RJ45乙太網端口？		v			
	150	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1.2.2	設備是否有可用的 USB 端口？		v			
	151	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1.2.3	設備是否需要、使用或支援可行動儲存設備？		v			
	152	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-1.2.4	設備是否支援其他實體連接？		v			
	153								
13.2	154	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-2	製造商是否提供設備使用或可能使用的網路端口和傳輸協定清單？ <TCP/UDP, 80, 21>	v				
13.3	155	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-3	設備能否與客戶環境中的其他系統連結通訊？		v			
13.4	156	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-4	設備能否與客戶環境外部的其他系統相通？（例如:AWS cloud）	v				
13.5	157	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-5	設備是否發出或接收 API 呼叫？	v				
13.6	158	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-6	設備是否需要網路連接才能用於其預期用途？		v		仍可量測血糖	
13.7	159	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-7	設備是否支援傳輸層安全 (TLS)？	v				
	160	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-7.1	TLS 可設定嗎？		v			
13.8	161	CONN-連接能力 (CONNECTIVITY CAPABILITIES, CONN)	CONN-8	該設備是否提供從另一個的設備能夠具有使用者控制功能？		v			
14		**PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)：設備鑑別認證使用者身份的能力**							
14.1	162	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-1	設備是否支援及強制所有系統帳號使用者與角色（包括服務帳號）使用個別獨一無二的 ID 和密碼？		v			
	163	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-1.1	設備是否強制所有系統帳號使用者與角色（包括服務帳戶）使用個別獨一無二的 ID 和密碼？			v		
14.2	164	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-2	設備是否可設定使用外部身分鑑別服務（例如 MS Active Directory、NDS、LDAP、OAuth 等）對系統帳號使用者進行身分鑑別？		v			
14.3	165	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-3	設備是否可設定讓系統帳號使用者嘗試登入失敗一定次數後即鎖定？	v				
14.4	166	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-4	文件中是否列出所有預設系統帳號（例如，技術人員服務帳戶、管理人員帳戶）？		v			
14.5	167	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-5	是否所有系統帳號使用者的密碼都可以被修改的？		v			
14.6	168	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-6	設備是否可設定當建立使用者帳號密碼必須強制滿足複雜性原則（各組織自行定義）？	v				
14.7	169	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-7	設備是否支援帳戶密碼週期性更新？	v				

14.8	170	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-8	設備是否支援多因子身分鑑別？		v			
14.9	171	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-9	設備是否支援單一登入 (SSO)？	v				
14.10	172	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-10	可以在設備上禁用/鎖定系統使用者帳戶嗎？		v			
14.11	173	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-11	設備是否支援生物特徵識別控制？	v				
14.12	174	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-12	設備是否支援實體權杖(physical tokens)（例如識別證存取）？		v			
14.13	175	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-13	設備是否支援群組鑑別（例如醫院團隊）？		v			
14.14	176	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-14	應用程式或設備是否儲存或管理身分鑑別憑證？		v			
	177	PAUT-使用者鑑別 (PERSON AUTHENTICATION, PAUT)	PAUT-14.1	憑證是否使用安全方法儲存？		v			
15		**PLOK-實體鎖 (PHYSICAL LOCKS, PLOK)：實體鎖可以防止對設備進行實體存取的未授權使用者損害儲存在設備或可移除式媒體上的使用者身分資訊的完整性和機密性**							
15.1	178	PLOK-實體鎖 (PHYSICAL LOCKS, PLOK)	PLOK-1	醫療器材是否為SaMD？如果是，請對本節中的其他問題進行回答“N/A”。		v			
15.2	179	PLOK-實體鎖 (PHYSICAL LOCKS, PLOK)	PLOK-2	醫療器材的所有元件是否使用實體鎖來保護使用者身分資訊（除了可移除式媒體）？（例如沒有實體鎖就無法刪除任何資料）<通用實體鎖>		v			
15.3	180	PLOK-實體鎖 (PHYSICAL LOCKS, PLOK)	PLOK-3	醫療器材的所有元件是否使用各自不同的實體鎖來保護使用者身分資訊（除了可移除式媒體）？	v				
15.4	181	PLOK-實體鎖 (PHYSICAL LOCKS, PLOK)	PLOK-4	設備是否可以讓客戶選擇實體鎖以限制對可移除式媒體的存取？			v		
16		**RDMP-設備在生命週期中第三方元件藍圖(ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE, RDMP)：廠商在設備生命週期內對第三方元件的安全支援計劃**							
16.1	182	RDMP-設備生命週期中第三方元件的路線圖(ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE, RDMP)	RDMP-1	在產品開發過程中是否遵循安全的軟體開發流程，例如 ：ISO/IEC 27034 或 IEC 62304？	v				
16.2	183	RDMP-設備生命週期中第三方元件的路線圖(ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE, RDMP)	RDMP-2	製造商是否於安全開發過程中，評估設備中所使用到的第三方應用程式和軟體元件？	v				
16.3	184	RDMP-設備生命週期中第三方元件的路線圖(ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE, RDMP)	RDMP-3	製造商是否有維護一個網頁或其他資訊管道來描述軟體更新日期與內容？	v				
16.4	185	RDMP-設備生命週期中第三方元件的路線圖(ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE, RDMP)	RDMP-4	製造商是否有管理第三方軟體元件終止的計劃？(Ex: winXP)			v		
17		**SBoM-軟體材料清單 (SOFTWARE BILL OF MATERIALS, SBoM)：軟體材料清單 (SBoM) 列出設備中所有整合描述的軟體元件，目的是醫療提供組織進行作業安全規劃。此部分支援 RDMP 部分中的控制項**							

17.1	186	SBoM-軟體材料清單 (SOFTWARE BILL OF MATERIALS, SBoM)	SBOM-1	是否有將該產品 SBoM 列出？	v				
17.2	187	SBoM-軟體材料清單 (SOFTWARE BILL OF MATERIALS, SBoM)	SBOM-2	SBoM 在描述軟體元件時是否遵循標準或通用方法？	v				
	188	SBoM-軟體材料清單 (SOFTWARE BILL OF MATERIALS, SBoM)	SBOM-2.1	是否識別出所有的軟體元件？	v				
	189	SBoM-軟體材料清單 (SOFTWARE BILL OF MATERIALS, SBoM)	SBOM-2.2	是否識別出所有的軟體元件的開發商與製造商？	v				
	190	SBoM-軟體材料清單 (SOFTWARE BILL OF MATERIALS, SBoM)	SBOM-2.3	是否識別出所有的軟體元件的主要版本編號？	v				
	191	SBoM-軟體材料清單 (SOFTWARE BILL OF MATERIALS, SBoM)	SBOM-2.4	是否識別出任何的附加說明？	v				
17.3	192	SBoM-軟體材料清單 (SOFTWARE BILL OF MATERIALS, SBoM)	SBOM-3	設備是否包含一種指令或程序方法來產生出設備上所被安裝的所有軟體元件列表？		v			
17.4	193	SBoM-軟體材料清單 (SOFTWARE BILL OF MATERIALS, SBoM)	SBOM-4	是否有針對SBoM 的更新流程？		v			
18		**SAHD-系統和應用程式的強化權限控制 (SYSTEM AND APPLICATION HARDENING, SAHD)：設備對網路攻擊和惡意軟體的防禦力**							
18.1	194	SAHD-系統和應用程式的權限強化控制 (SYSTEM AND APPLICATION HARDENING, SAHD)	SAHD-1	設備是否有按照任何工業標準對網路攻擊和惡意軟體進行強化？	v				
18.2	195	SAHD-系統和應用程式的權限強化控制 (SYSTEM AND APPLICATION HARDENING, SAHD)	SAHD-2	該設備是否已獲得任何網路安全驗證？	v				
18.3	196	SAHD-系統和應用程式的權限強化控制 (SYSTEM AND APPLICATION HARDENING, SAHD)	SAHD-3	設備是否採用任何軟體完整性檢查機制	v				
	197	SAHD-系統和應用程式的權限強化控制 (SYSTEM AND APPLICATION HARDENING, SAHD)	SAHD-3.1	設備是否採用任何機制（例如，特定於版本的hash密鑰、校正和數位簽章等）來確保安裝的軟體是由製造商授權的？	v				
	198	SAHD-系統和應用程式的權限強化控制 (SYSTEM AND APPLICATION HARDENING, SAHD)	SAHD-3.2	設備是否採用任何機制（例如，特定於版本的雜湊密鑰、校正和數位簽章等）來確保軟體更新是由製造商授權的？	v				
18.4	199	SAHD-系統和應用程式的權限強化控制 (SYSTEM AND APPLICATION HARDENING, SAHD)	SAHD-4	擁有者/使用者能否自行執行軟體完整性檢查（即，驗證系統未被修改或篡改）？	v				
18.5	200	SAHD-系統和應用程式的權限強化控制 (SYSTEM AND APPLICATION HARDENING, SAHD)	SAHD-5	系統是否可設定為允許實施檔案分級、病患分級或其他類型的存取控制？	v				
	201	SAHD-系統和應用程式的權限強化控制 (SYSTEM AND APPLICATION HARDENING, SAHD)	SAHD-5.1	設備是否提供基於身分的存取控制？		v			
18.6	202	SAHD-系統和應用程式的權限強化控制 (SYSTEM AND APPLICATION HARDENING, SAHD)	SAHD-6	在系統交付時，製造商是否可限制或禁用某些系統或使用者帳戶？		v			
	203	SAHD-系統和應用程式的權限強化控制 (SYSTEM AND APPLICATION HARDENING, SAHD)	SAHD-6.1	初始化後，終端使用者是否可以設定系統或使用者帳戶？		v			

	204	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-6.2	是否包括將某些系統或使用者帳戶（例如服務技術人員）限制至僅具有最低存取權限？		v			
18.7	205	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-7	是否禁用設備上非必要的共享資源（例如檔案分享）？	v				
18.8	206	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-8	是否禁用設備上非必要的通訊埠和通訊協定？			v		
18.9	207	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-9	是否刪除/禁用設備非必要用途的所有服務（例如，telnet、檔案傳輸協定[FTP]、互聯網資訊伺服器 [IIS] 等）？			v		
18.10	208	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-10	是否刪除/禁用設備非必要用途的所有應用程序（COTS 應用程序以及包含作業系統的應用程式，例如 MS Internet Explorer 等）？			v		
18.11	209	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-11	設備能否禁止從無法控制或可移除式媒體（即內部驅動程式或內部儲存元件以外的來源）啟動？			v		
18.12	210	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-12	可以在不使用實體工具的情況下在設備上安裝未經授權的軟體或硬體嗎？	v				
18.13	211	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-13	產品文件是否包含使用者操作網路安全掃描的資訊？		v			
18.14	212	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-14	設備是否可以在預設提供的狀態之外進行對網路攻擊和惡意軟體的防禦力強化？		v			
	213	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-14.1	經銷商是否提供有關對網路攻擊和惡意軟體的防禦力強化的說明？		v			
18.15	214	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SHAD-15	系統能否在開機期間避免外部存取BIOS 或其他開機程序？		v			
18.16	215	SAHD-系統和應用程式的權限強化控制（SYSTEM AND APPLICATION HARDENING, SAHD）	SAHD-16	是否使用未包含在 SAHD2.3.19 中的其他強化方法來強化設備對網路攻擊和惡意軟體的防禦力？		v			
19		**SGUD-安全指南（SECURITY GUIDANCE, SGUD）：安全指南提供設備上作業人員和管理員以及廠商的銷售和服務**							
19.1	216	SGUD-安全指南（SECURITY GUIDANCE, SGUD）	SGUD-1	設備是否包括擁有者/使用者之安全指南？	v				
19.2	217	SGUD-安全指南（SECURITY GUIDANCE, SGUD）	SGUD-2	設備是否具有從設備或媒體中永久刪除資料的能力並提供說明？	v				
19.3	218	SGUD-安全指南（SECURITY GUIDANCE, SGUD）	SGUD-3	是否有在安全指南上列出所有可存取的帳戶？	v				
	219	SGUD-安全指南（SECURITY GUIDANCE, SGUD）	SGUD-3.1	擁有者/使用者可以管理所有帳戶的密碼設定嗎？		v			
19.4	220	SGUD-安全指南（SECURITY GUIDANCE, SGUD）	SGUD-4	產品是否包含有關建議的設備補償控制文件嗎？		v			

20		**STCF-醫療資料儲存機密性 (HEALTH DATA STORAGE CONFIDENTIALITY, STCF)：設備確保未經授權存取功能不會損害儲存設備或可移除式媒體上的使用者身分資訊之完整性和機密性**							
20.1	221	STCF-醫療資料儲存機密性 (HEALTH DATA STORAGE CONFIDENTIALITY, STCF)	STCF-1	設備可以加密靜態資料嗎？	v				
	222	STCF-醫療資料儲存機密性 (HEALTH DATA STORAGE CONFIDENTIALITY, STCF)	STCF-1.1	所有資料是否加密或以其他方式受到保護？	v				
	223	STCF-醫療資料儲存機密性 (HEALTH DATA STORAGE CONFIDENTIALITY, STCF)	STCF-1.2	是否有預設資料加密功能？	v				
	224	STCF-醫療資料儲存機密性 (HEALTH DATA STORAGE CONFIDENTIALITY, STCF)	STCF-1.3	客戶是否擁有設定加密之說明？		v			
20.2	225	STCF-醫療資料儲存機密性 (HEALTH DATA STORAGE CONFIDENTIALITY, STCF)	STCF-2	可以更改或設定加密密鑰嗎？		v			
20.3	226	STCF-醫療資料儲存機密性 (HEALTH DATA STORAGE CONFIDENTIALITY, STCF)	STCF-3	資料是否儲存在設備上的資料庫中？	v				
20.4	227	STCF-醫療資料儲存機密性 (HEALTH DATA STORAGE CONFIDENTIALITY, STCF)	STCF-4	資料是否儲存在設備外部的資料庫中？	v				
21		**TXCF-傳輸機密性 (TRANSMISSION CONFIDENTIALITY, TXCF)：設備確保傳輸使用者身分資訊的機密性能力**							
21.1	228	TXCF-傳輸機密性 (TRANSMISSION CONFIDENTIALITY, TXCF)	TXCF-1	能否僅通過點對點專用電纜傳輸使用者身分資訊？		v			
21.2	229	TXCF-傳輸機密性 (TRANSMISSION CONFIDENTIALITY, TXCF)	TXCF-2	使用者身分訊息通過網路或可移除式媒體傳輸之前是否有加密？	v				
	230	TXCF-傳輸機密性 (TRANSMISSION CONFIDENTIALITY, TXCF)	TXCF-2.1	如果資料預設不加密，客戶可以設定加密選項嗎？					
21.3	231	TXCF-傳輸機密性 (TRANSMISSION CONFIDENTIALITY, TXCF)	TXCF-3	使用者身分資訊傳輸是否僅限於固定的網路目的端名單？	v				
21.4	232	TXCF-傳輸機密性 (TRANSMISSION CONFIDENTIALITY, TXCF)	TXCF-4	所有的連接是否均必須通過身分驗證系統？	v				
21.5	233	TXCF-傳輸機密性 (TRANSMISSION CONFIDENTIALITY, TXCF)	TXCF-5	是否支援/採取某些既有安全傳輸方法 (Ex: DICOM、HL7、IEEE 11073) ？		v			
22		**TXIG-傳輸完整性 (TRANSMISSION INTEGRITY-TXIG)：設備確保傳輸資料完整性的能力**							
22.1	234	TXIG-傳輸完整性 (TRANSMISSION INTEGRITY-TXIG)	TXIG-1	設備是否支援確保任何資料在傳輸過程中不被修改的機制（例如，數位簽章）？		v			
22.2	235	TXIG-傳輸完整性 (TRANSMISSION INTEGRITY-TXIG)	TXIG-2	設備是否包含通過外部電纜連接的多個子元件？		v			

23		RMOT-遠端服務（REMOTE SERVICE, RMOT）：遠端服務是指服務人員通過網路或其他遠端連接進行的各種設備維護活動							
23.1	236	RMOT-遠端服務（REMOTE SERVICE、RMOT）	RMOT-1	設備是否允許遠端服務連接以進行設備分析或維修		v			
	237	RMOT-遠端服務（REMOTE SERVICE、RMOT）	RMOT-1.1	設備是否允許擁有者/使用者開啟遠端服務以進行設備分析或維修？			v		
	238	RMOT-遠端服務（REMOTE SERVICE、RMOT）	RMOT-1.2	是否提供遠端存取開啟與進行中的標示/提醒？			v		
	239	RMOT-遠端服務（REMOTE SERVICE、RMOT）	RMOT-1.3	在遠端存取期間可以存取或查看裝置上的病患資料嗎？			v		
23.2	240	RMOT-遠端服務（REMOTE SERVICE、RMOT）	RMOT-2	設備是否允許或使用遠端服務連接來獲取預測性維護資料？			v		
23.3	241	RMOT-遠端服務（REMOTE SERVICE、RMOT）	RMOT-3	設備是否具有任何其他遠端存取功能（例如軟體更新、遠端訓練）？			v		