衛生福利部醫療領域資通系統資安防護基準

一、依據

衛生福利部(以下簡稱本部)為資通安全管理法醫療領域特定非公務機關之中央目的事業主管機關，就該特定領域類型資通系統有另為規定防護基準之必要，爰依資通安全責任等級分級辦法第11條第2項後段規定，訂定本防護基準，供醫院資通系統實施各項資安防護控制措施之依循。

二、適用範圍

本防護基準適用範圍為依資通安全管理法受本部轄管之醫療領域之特定非公務機關。

醫療儀器資通系統與其他支援設施資通系統應依循機關之資安維護計畫，涉及相關組織及委外管理等要項，須依循機關之資安管理框架。

三、用詞定義：

(一)資安列管醫療儀器：指放置院區內場域，有對外連線網際網路（Internet）或連結院內系統網路(Intranet)，或具網路位址(IP)追蹤性，或交換資料間接上傳醫療相關資訊系統(如:PACS、HIS)等之臨床使用醫療終端儀器及控制系統。

(二)醫療資訊系統(Healthcare Information System,HIS)：指傳統醫療資訊業務管轄之臨床資訊應用系統，包含資料庫及後端處理臨床表單之系統。

(三)醫療影像儲傳系統(Picture archiving and communication system,PACS)：包含OT之影像擷取組像及上傳元件端與IT之醫療影像傳輸儲存及調閱系統端二部份；元件端，為具醫療數位影像傳輸協定(DICOM Module)醫療儀器的集合，系統端，含醫師醫囑項目與照攝影像及報告資訊。

(四)醫療儀器資通系統：泛指資安列管醫療儀器之控制系統分群、終端儀器分群之邊界主機，參考「醫療儀器資安分群分類模型」範圍。

(五)醫療物聯網裝置（The Internet of Medical Things,IoMT）：泛指藉由物聯網(The Internet of Things,IoT)技術進行資料蒐集或傳輸之設備。

(六)邊界主機：指管理獨立網域內網(Local LAN)運作之儀器群組主機，並隔離介接院內系統網路(Intranet)之具網路區隔功能閘道器或伺服主機(如:雙網卡 Edge Gateway 或 Device Server)。

(七)儀器獨立網域內網(Local LAN)：指儀器群組(為：「群組型儀器」或「系統型儀器」)依儀器原廠建議或工控區(OT Zone)資安防護目的，所規劃及佈建的獨立網域內網，以確保穩定性、安全性需求；或稱「設備內網」、「內內網」。

(八)儀器獨立網段：指院內系統網路(Intranet)網域，分割隔離網段後，規劃獨立於行政電腦網段外，專屬予醫療儀器運行使用之網段。

(九)OT 防火牆:對比於資通區(IT Zone)介接網際網路(Internet)的「醫院外部防火牆」名詞，指醫院內部「資安列管類醫療儀器」分區佈建後，介接院內系統網路(Intranet)的醫療儀器跨區防火牆。

四、醫療儀器資安分群分類

(一)機關盤點具連網功能的醫療儀器資產，應涵蓋「資安列管醫療儀器」之範圍。

(二)「資安列管醫療儀器」依「元件」與「系統」資料流之從屬關係特性，作為「分群」依循，為「終端儀器」與「控制系統」二群；依資料流來源至目的 IP 之跨區軌跡，作為「分類」依循，二群分五類(如附圖一)；透過「醫療儀器資安分群分類模型」模型化分群分類，防護標的實施普、中、高分級的控制措施項目。

(三)終端儀器群：指臨床上使用之醫療儀器，經連結院內系統網路(Intranet)傳輸資料之儀器設備或醫療儀器，包含三類：「終端單機」、「群組型儀器」及「系統型儀器」。

1.終端單機：指臨床使用直接連結院內系統網路(Intranet)傳輸資料至資通區(IT Zone)中繼邊界 Gateway 之單機型醫療儀器。如：超音波影像儀為單機型醫療儀器，傳輸資料連結 PACS 系統之工作清單 Gateway、DICOM 影像 Gateway。

2.群組型儀器：指多台功能相同之醫療儀器組成獨立網域內網(Local LAN)，透過隔離措施間接進行單機院內系統網路(Intranet)連線之「內網邊界主機」。如：ICU 生理監視器群組的

中央站、內網化連網洗腎機群組的邊界主機(Edge Loader Gateway)。

3. 系統型儀器：指由不同功能模組單機在獨立網域內網(Local LAN)組合而成一套醫療儀器，透過隔離措施間接進行單機院內系統網路(Intranet)連線之內網邊界主機；或指使用於臨床獨立網域內網(Local LAN)，多台功能不相同模組單機組合而成一套醫療儀器的「邊界主機」，經隔離間接連結院內系統網路(Intranet)。

如：MRI、CT、PET 連結 PACS 系統的介面控制台 console。

(四)控制系統群：指規格上可連線管理2台（含）以上「終端儀器」群之終端單機或邊界主機，連結院內系統網路(Intranet)傳輸資料之臨床儀器控制系統，包含「醫儀控制系統」與「醫儀應用系統」二類。

1. 醫儀控制系統：全稱為「醫療儀器資訊控制系統」，指控制「終端儀器」非人類連線的管理系統(Device Server)；只管理「儀器ID」及「檢驗檢查資料」；不落地儲存與醫療相關資訊系統交換的「可識別資料」、不管理資料查詢的「醫事人員帳密權控」；功能上不涉及識別個人資訊的控制軟體系統。如：ICU 生理監護系統伺服器主機、洗腎機拋轉系統設備伺服器的控制軟體系統。

2. 醫儀應用系統：全稱為「醫療儀器資訊應用系統」，指「終端儀器」的控制應用管理系統(AP Server)；包含交換且儲存 HIS 病人個資資訊、提供臨床人員查詢報告等服務，有管理醫事人員帳密權控等可識別資訊的儀器控制及連結臨床應用套裝軟體系統。

如：產房資訊系統、檢驗備管系統伺服器的應用軟體系統。

五、機關資通系統適用規定

(一)機關自行或委外開發之資通系統，應依「資通安全責任等級分級辦法」第11條附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施。

(二)醫療儀器應符合「醫療器材管理法」及相關子法與「醫療器材品質管理系統準則」之衛生福利部許可證相關安規驗證規定;另「資安列管醫療儀器」終端儀器群邊界主機與控制系統群為醫療儀器資通系統防護基準之防護標的，應依本防護基準附表一執行控制措施。

(三)其他支援設施之特定類型資通系統，執行「資通安全責任等級分級辦法」第11條附表十所定控制措施，因技術限制、系統設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得參考其他領域公告之相關資通或工控系統之控制措施。

六、醫療儀器資料流管理

(一)「資安列管醫療儀器」分群分類之醫療儀器，依資安風險區劃 ZCR 方法，評估分區「防護需求等級(SL)」、規劃「網路安全區塊(Zone)」分區、建立跨區資料傳輸「安全管道(Conduit)」；ZCR 網路規劃參考公用之醫療儀器資料流網路模板(Template)。(如附圖二)

(二)資安風險區劃(Zone, conduit and risk assessment,ZCR)：「資安列管醫療儀器」分群分類之醫療資料流，依評估資安需求等級 SL(Security Level)規劃建立「網路安全區塊(Zone)」分區；跨區管道(Conduit)佈建資料流通道之過濾阻擋「控制項」防護機制，達到：受攻擊面縮小(Attack Surface Reduction)、縱深防禦(Defense in Depth)等防護效果之資安風險管理實作流程。

(三)資安防護需求等級(Security Level,SL)：針對「控制系統」依據資通系統防護需求分級原則，評估機密性(C)、完整性(I)、可用性(A)、法遵性(L)各構面之分級取最高等級者，評估「資產價值」，評定普、中、高之「資安防護需求等級」，簡稱 SL(Security Level)；SL 由低至高分級為 SL(0)~SL(4)對應資安防護需求普、中、高等級。

1.SL(0)：指「信任連線」。

2.SL(1)~ SL(2)：資安防護需求等級普級。

3.SL(3)為：資安防護需求等級中級。

4.SL(4)為：資安防護需求等級高級。

(四)信任連線：指經風險評鑑後，風險可承受範圍內的短距離機器連線資料傳輸；對應防護需求等級為 SL(0)；安全(Safety)議題另受醫療法規「醫療器材管理法」規範。

(五)網路安全區塊(Zone)：指「資安列管醫療儀器」之建置，網路規劃上的資料流資安防護需求分區，可分「網際網路(Internet)」、「院內系統網路(Intranet)」、「工控區(OT Zone)」、「信任連線」區塊(包含:儀器獨立網域內網(Local LAN)、RS232連線、藍芽、RF、IR…等低風險短距連線)。每一區塊，透過資安風險評估資安防護需求等級(SL)，每一資安風險區塊(Zone)內之資安列管儀器列為相同 SL；「子區塊」之 SL≦「母區塊」。

(六)管道(Conduit)：泛指跨「網路安全區塊(Zone)」之間，經套用對應跨區等級「控制項」防護機制(如：資料流經隔離、清洗、阻擋)後，之安全資料傳輸通道。

七、醫療儀器資通系統資安風險評估與檢討改善

(一)本防護基準「醫療儀器資料流網路模版」，提供機關確認「終端儀器群」與「控制系統群」之醫療資訊資料流、清查連網方式、連網儀器及所介接系統，依分區完成資安風險評估，並執行對應控制措施。

(二)資產風險改善

在套用「控制措施」後，依據可能發生的外部事件影響風險構面，每年針對「資安列管儀器」，經選擇適用規範之「風險識別」、「風險分析」與「衝擊分析」等風險評估工具與方法論，逐年檢討「資安風險等級(Cyber Risk Level,CRL)」之低、中、高等級，改善資安風險。

1.高：不可接受(Unacceptable)。

2.中：可能接受的(Potentially Acceptable)。

3.低：可接受的(Acceptable)。

八、實作指引

為協助機關落實本防護基準，逐年完備機關之醫療儀器資安防護控制措施，由本部另行公告「醫療儀器資通系統資安防護作業實作指引」，供醫院導入實務運作參考。

附表一 醫療儀器資通系統資安防護基準

控制項		系統防護需求分級		資安列管醫療儀器防護標的	
控制構面	控制目標	分級	控制措施	終端儀器群之邊界主機	控制系統群
網路架構	網段規劃	高	一、規劃院內 OT 防火牆，並有對應控制系統之網路管控措施(如: 網路封包過濾功能、支援之工控協定等)。 二、等級「中」之所有控制措施。	■	■
		中	一、規劃儀器獨立網段網路與院內系統網路區隔，並有跨區(Zone)院內 OT 防火牆連網政策規則。 二、等級「普」之所有控制措施。	■	■
		普	一、「群組型儀器」、「系統型儀器」，應適當區域內網化規劃。 二、在「院內系統網路」與「儀器獨立網域內網」網絡跨區(Zone)架設院內 OT 防火牆或採取風險控制補償措施。	■	■
	邊界防護	高中	一、監視「控制系統」外部邊界與關鍵內部邊界之通訊。 二、等級「普」之所有控制措施。		■
		普	「邊界主機」、「控制系統」網絡「邊界主機」應採取防護具體措施，並定期審查防護措施。	■	■
存取控制	帳號管理	高	一、定期盤點帳號並審核，並有相關異常管理機制。 二、等級「中」之所有控制措施。		■
		中	一、已不被授權(如：離職或調任)之帳號予以刪除或停用。 二、帳號定期變更密碼。 三、等級「普」之所有控制措施。		■
		普	一、「終端儀器」有原廠預設帳密應變更預設密碼，如無法更改應有其他補償措施。 二、「控制系統」工作站/伺服器作業系統應變更原廠預設帳號密碼；儀器原廠無法變更者，應有資安管理作業程序。 三、「控制系統」非合法權控帳號定期點檢。 四、「醫儀應用系統」依循醫院規定之帳號管理機制，且不得使用共用帳號。	■	■
	遠端存取	高中普	一、應依循醫院規定遠端存取管理規範，包含連線需求申請、使用限制與使用者權限檢查等作業並留存記錄。 二、醫院遠端存取，應有時效性限制及「院內系統網路(Intranet)」監控機制。	■	■

控制項		系統防護需求分級		資安列管醫療儀器防護標的	
控制構面	控制目標	分級	控制措施	終端儀器群之邊界主機	控制系統群
	最小權限	高 中 普	臨床使用者開機權限應採最小權限原則，僅開放使用者必要之授權存取及應用；儀器原廠無法變更者，應有其他補償措施。	■	■
	無線網路管理	高 中	一、「資安列管醫療儀器」及「IoMT」依特性及使用目的，分網路安全區塊(Zone)設置 Wi-Fi 無線網路熱點(SSID)，配置對等之資安防護措施以連線「院內系統網路(Intranet)」 二、等級「普」之所有控制措施。	■	■
		普	一、「資安列管醫療儀器」及「IoMT」的使用，其 Wi-Fi 無線網路建立相關區隔網段與存取權限授權，應依循「院內系統網路(Intranet)」之管理規範。 二、限制 Wi-Fi 無線連網儀器和院內核心網路之間的資料交換。 三、實作「儀器獨立網域內網(Local LAN)」Wi-Fi 無線網路熱點(SSID)安全機制。	■	■
事件日誌與可歸責性	事件記錄	高 中	一、應定期審查所保留產生之日誌，並保留日誌至少六個月，如無日誌紀錄供審查應有其他補償措施。 二、等級「普」之所有控制措施		■
		普	「邊界主機」、「醫儀控制系統」、「醫儀應用系統」，留有適當之日誌紀錄，如無法留存日誌紀錄應有其他補償措施。	■	■
	日誌紀錄內容	高 中	一、確保日誌紀錄格式至少應包含發生事件、發生時間、使用者等追蹤資訊。 二、等級「普」之所有控制措施。		■
		普	系統日誌紀錄功能內容應有明確記錄欄位資訊，如無結構紀錄應有其他補償措施。	■	■
	日誌儲存容量	高 中 普	配置適當日誌紀錄的儲存容量。	■	■
	日誌處理失效之回應	高 中 普	日誌處理失效時應採取適當之行動。	■	■
	時戳	高 中	一、系統內部時鐘應定期與基準時間源進行同步。 二、等級「普」之所有控制措施。		■
		普	時間定期(手/自動)校時或同步機制。	■	■
	日誌資訊之保護	高 中	一、日誌紀錄有備份保存管理機制。 二、等級「普」之所有控制措施。		■

控制項		系統防護需求分級		資安列管醫療儀器防護標的	
控制構面	控制目標	分級	控制措施	終端儀器群之邊界主機	控制系統群
		普	日誌紀錄有存取權限管理，對日誌之存取僅限於有權限之使用人員，以防護日誌資訊之完整性。	■	■
營運持續計畫	營運持續計畫	高中	一、應有系統備份機制並確認備份完整性且有備份復原機制。 二、等級「普」之所有控制措施。		■
		普	一、臨床使用應訂有臨床業務營運持續計畫，於可容忍時間內替代流程提供服務，並執行演練。 二、定期審查營運持續計畫，以維持臨床服務之可用性與病人安全。	■	■
	安全模式	高中	一、「醫儀控制系統」、「醫儀應用系統」系統安全模式操作，可以自動或手動啟動，如危及安全時有手動或自動暫時替代 bypass 功能。 二、等級「普」之所有控制措施。		■
		普	一、「資安列管醫療儀器」依循醫院限制或防止入侵者存取的安全機制(如：封鎖單機 IP 或暫時離線機制)。 二、「終端儀器」可離線單機運作。	■	■
	控制系統備援	高中	一、具有進階備援機制。 二、等級「普」之所有控制措施。		■
		普	「邊界主機」、「控制系統」之儀器伺服器主機具有持續營運機制。	■	■
識別與鑑別	內部使用者之識別與鑑別	高中普	依循醫院帳號及權控管理機制建立內部一般使用者、最高管理者及廠商等帳號管理；如無法單一識別使用者時，須有替代監管措施，如排班表、影像紀錄等。		■
	裝置之識別與鑑別	高中	一、「醫儀控制系統」與「醫儀應用系統」應識別與鑑別連接至系統之「終端儀器」，及擁有終端儀器管理機制，如無法識別與鑑別連接之「終端儀器」應有其他補償措施。 二、等級「普」之所有控制措施。	■	■
		普	連結「院內系統網路」儀器，應依循醫院申請審核流程與網管 IP 配發作業規範。	■	■
	身分鑑別管理	高中普	一、應有帳戶識別機制，如無法單一使用者鑑別時，須有替代管理措施，如使用者值排、排班紀錄等鑑別使用者。 二、「醫儀應用系統」身分驗證應依循醫院帳號管理規則(如：納入醫院單一登錄系統)；若系統無法依循醫院帳號管理規則，須有其他補償管理措施。	■	■
	鑑別資訊	高	應遮蔽在鑑別過程中之資訊。	■	■

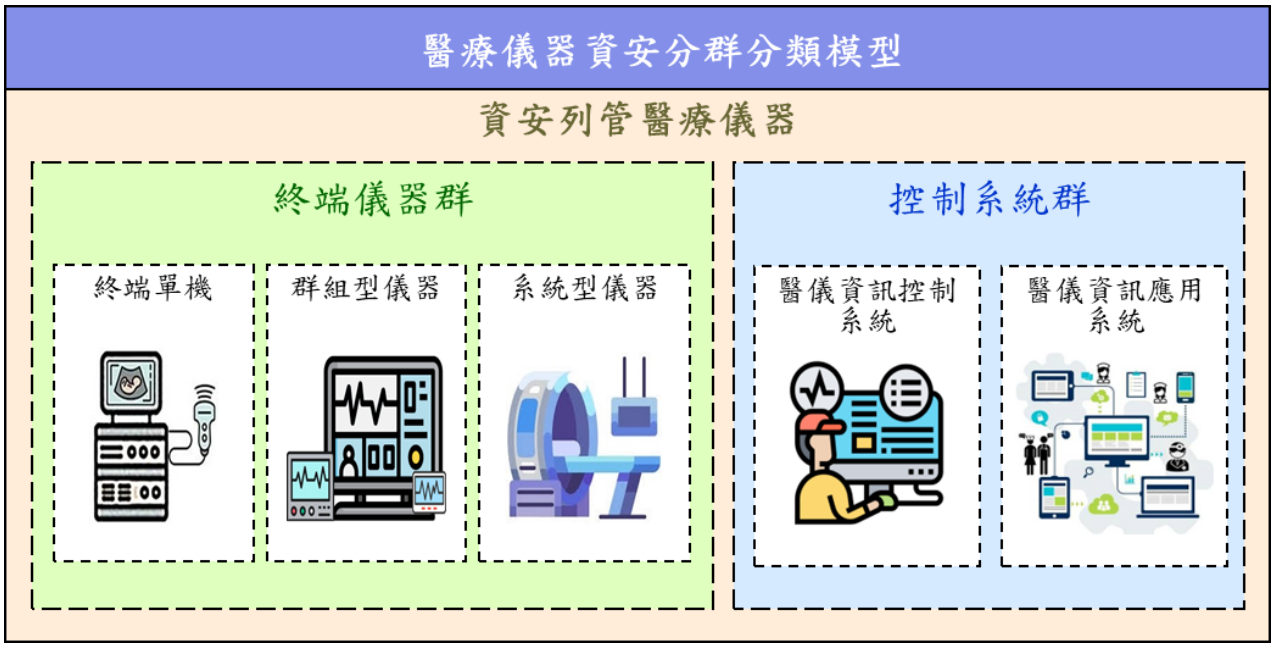
控制項		系統防護需求分級		資安列管醫療儀器防護標的	
控制構面	控制目標	分級	控制措施	終端儀器群之邊界主機	控制系統群
	回饋	中 普			
系統與通訊防護	傳輸之機密性與完整性	高 中	一、設定院內 OT 防火牆只允許儀器跨區(Zone)傳輸資料之伺服器、工作站、合法傳輸點 IP 之白名單路由。 二、院內 OT 防火牆只開啟儀器需使用之網路通訊服務埠。 三、等級「普」之所有控制措施。	■	■
		普	連線「院內系統網路(Intranet)」終端儀器邊界主機或控制系統伺服器主機，應有邏輯隔離或實體隔離，如無法邏輯隔離或實體隔離應有其他補償措施。	■	■
	資料儲存之安全	高 中 普	系統、應用程式組態備份靜置資訊之儲存媒體裝置，應予以防護。	■	■
系統與服務獲得	外部系統服務	高 中	一、外部之服務供應商(Service Provider)、系統整合商(System Integrator)應提供系統資安證明文件(如：第三方安全性檢測證明)，涉及使用非自行開發之系統或資源者，應標示非自行開發之內容與其來源及授權證明。 二、等級「普」之所有控制措施。		■
		普	「邊界主機」、「控制系統」之供應商(Product Supplier)、系統整合商(System Integrator)或服務供應商(Service Provider)所提供之外部系統服務，應將資安要求納入醫院制式契約並要求服務供應商確實遵守。	■	■
	系統文件	高 中 普	定期審查資訊安全管理系統相關文件、更新紀錄；存檔管理醫療儀器相關驗收文件。	■	■
實體與環境防護	實體(儀器使用者)存取授權	高 中 普	置放場域相關使用者授權應審查符合醫院醫療照護相關規範(如：醫院評鑑)，進出置放場域須有授權人員管控(如：配戴證件、分組班表、動線出入口 CCTV)，變更時亦同。	■	■
	實體(儀器門禁)進出控制	高	一、伺服器主機應有獨立機房及環控設施，如：設置於中央資訊機房。 二、等級「中」之所有控制措施。		■
		中	一、設施所在區域有實體隔離機制，置放場域經授權人員進出管理與紀錄(如：授權人員門禁刷卡紀錄)。 二、等級「普」之所有控制措施。	■	■
		普	置放場域應符合醫院醫療照護相關環境安全規範(如：醫院評鑑)，置放場域需有授權人員進出管制機制。	■	■

控制項		系統防護需求分級		資安列管醫療儀器防護標的	
控制構面	控制目標	分級	控制措施	終端儀器群之邊界主機	控制系統群
	緊急電源	高中	一、即時替代電力供應，系統儀器主機應有專用或中央不斷電 UPS 供電。 二、等級「普」之所有控制措施。		■
		普	「邊界主機」、「控制系統」建立能供應最小業務負載量之長時間緊急發電電力備援機制，符合醫院醫療照護相關環境安全規範(如：醫院評鑑)，並有定期公共安全查檢。	■	■
	實體公用服務備援	高中普	「資安列管醫療儀器」置放場域公用服務(如水、氣、空調、消防及通訊等環境動力源)應有備援機制，並依循定期公共安全查檢。	■	■
	實體危害因素控制	高中普	一、置放場域之環境應依循醫院危害因素控制管理規範，符合儀器規格之危害因素防護要求(依原廠規範，如：對於溫溼度控制、水損、火、煙、水、震動、化學效應、電力供應、電磁、輻射或人為入侵破壞等危害因素)。 二、置放場域之環境應依循醫院危害因素控制管理規範與定期公共安全查檢，並符合「原子能法」、「游離輻射防護法」輻防管制法令規範。	■	■
	第三方/陪同者的存取	高中	一、「醫儀控制系統」與「醫儀應用系統」非醫院人員存取，須有院方人員陪同與記錄機制。 二、等級「普」之所有控制措施。		■
		普	「邊界主機」、「控制系統」置放場域非醫院人員存取應依循醫院人員實體存取安全控制管理規範，包含人員進出管理、可攜式行動資訊設備存取管理與其他有關醫院資安要求。	■	■
系統與資訊完整性	漏洞修補	高	一、針對具資安風險之漏洞或軟體，在儀器原廠許可下，對具資安風險之漏洞進行修補或軟體更新，並完成測試，或採取補償性控制措施來避免資安風險。 二、針對終端儀器邊界主機及控制系統伺服器，每年排程弱點掃描。 三、等級「中」之所有控制措施。	■	■
		中	一、加強醫療儀器外部資安情資蒐集分析與因應控制措施。 二、等級「普」之所有控制措施。	■	■
		普	在儀器原廠許可下，針對具資安風險之漏洞或軟體更新，或採取補償性控制措施，以降低資安風險。	■	■

控制項		系統防護需求分級		資安列管醫療儀器防護標的	
控制構面	控制目標	分級	控制措施	終端儀器群之邊界主機	控制系統群
	惡意程式防護	高中	一、控制系統應有偵惡意程式防護機制，如無法佈署惡意防護工具應有其他型式對策(如：加強 USB 惡意程式掃描等)或採取補償性控制措施來避免資安風險。 二、控制系統應納入全院 Intranet 網路安全監控機制，並有警訊通報或回饋機制；如無法納入全院網路安全監控應有其他補償措施。 三、等級「普」之所有控制措施。		■
		普	應實作降低弱點暴露應因應對策，控制系統或儀器主機應在儀器原廠許可下安裝防毒軟體，如無法佈署惡意防護工具應有其他補償措施(如：醫院內部 OT 防火牆對應控制系統之防護政策等)。		■
	系統監控	高中普	監控工具在不影響控制系統操作可用性下，納入「院內系統網路」系統監控回饋機制(如：SOC、SIEM 等 IT 資安監控工具）；如無法納入應有其他補償措施。	■	■
	可預測之故障預防	高中	一、建立故障預防機制，分析系統可靠度與潛在故障因素(如平均故障時間、故障原因分析等)，及早因應。 二、等級「普」之所有控制措施。		■
		普	建立系統維護紀錄管理機制，並符合醫院醫療照護相關環境安全規範(如醫院評鑑)，包含定期維護、檢查、測試、保養或校正作業，並有紀錄可查。	■	■
	故障容許度	高中	一、評估重要組件容錯機制(如：終端設備斷線儲存/連線重傳機制、使用隔離抗干擾網路線材、昇級安全通訊協定等)，提升控制系統資安韌性，進行防護措施，如無法評估或經評估無法提供防護應有適當措施。 二、等級「普」之所有控制措施。		■
		普	遵循「醫療器材管理法」法令規範建立通報機制，ADR 不良品及不良反應通報系統通報回饋製造商以持續改善產品。	■	■
組態管理	組態變更控制	高中	一、建立組態變更管理機制（如：變更申請流程、維修工單作業紀錄文件化)。 二、等級「普」之所有控制措施。		■
		普	一、系統初始安裝期間，若設定非原廠之預設功能組態時，應有組態還原機制(如：組態設定紀錄、組態備份)。 二、系統營運期間組態變更時，應文件化保留變更紀錄。	■	■
	最基本功能	高中普	依儀器原廠手冊安裝程序組態設定，系統設定時，僅提供業務必要的最小功能(如：關閉連外瀏覽器、只可安裝原廠已授權之第三方軟體)。	■	■

註：防護需求控制措施防護需求說明及實務操作指引,可參考「醫療儀器資通系統資安防護作業實作指引」。

附圖一、醫療儀器資安分群分類模型



一、「資安列管醫療儀器」依「元件」與「系統」特性，分為「終端儀器」與「控制系統」二群。

二、「終端儀器」群包含三類:「終端單機」、「群組型儀器」、「系統型儀器」。

三、「控制系統」群包含二類:「醫療儀器資訊控制系統類」、「醫療儀器資訊應用系統類」。

附圖二、醫療儀器資料流網路模板

【醫療儀器資訊網路基本架構圖公用參考範例】