正本

檔　　號：
保存年限：

衛生福利部食品藥物管理署　函

機關地址：11561 臺北市南港區昆陽街161-2號
傳　　真：
聯絡人及電話：簡俊仁2787-7551
電子郵件信箱：

241
新北市三重區重新路五段609巷6號3樓之3

受文者：台灣醫療暨生技器材工業同業公會

台灣醫療暨生技器材工業同業公會
收 110. 05. 06 文
檔號: 110366

發文日期：中華民國110年5月3日
發文字號：FDA器字第1101603501號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：「適用於製造業者之醫療器材網路安全指引」業經本署於110年5月3日以FDA器字第1101603391號公告，請查照並轉知所屬。

說明：旨揭公告及其附件請至本署全球資訊網站(網址：http://www.fda.gov.tw)之公告區及醫療器材法規專區自行下載。

正本：新北市醫療器材商業同業公會、台灣醫療器材門市發展協會、台灣醫療暨生技器材工業同業公會、中華民國醫療器材商業同業公會全國聯合會、臺北市醫療器材商業同業公會、桃園市醫療器材商業同業公會、臺中市醫療器材商業同業公會、彰化縣醫療器材商業同業公會、嘉義市醫療器材商業同業公會、台南市直轄市醫療器材商業同業公會、臺南市醫療器材商業同業公會、高雄市醫療器材商業同業公會、台灣省醫療器材商業同業公會聯合會、屏東縣醫療器材商業同業公會、高雄市直轄市醫療器材商業同業公會、台灣口腔生物科技暨醫療器材產業發展促進協會、台灣牙科器材同業交流與公益協會、台北市生物技術服務商業同業公會、社團法人中華民國助聽器同業聯合協進會、中華民國助聽器商業同業公會全國聯合會、台北市助聽器商業同業公會、桃園縣助聽器商業公會、台中市助聽器商業同業公會、彰化縣助聽器商業同業公會、高雄市助聽器商業同業公會、中華民國眼鏡發展協會、台灣區眼鏡工業同業公會、台北市眼鏡商業同業公會、台灣省鐘錶眼鏡商業同業公會聯合會、高雄市鐘錶眼鏡商業同業公會、台灣生技醫療照護輔具協會、社團法人臺灣輔具產業發展協會、中華民國儀器商業同業公會全國聯合會、臺北市儀器商業同業公會、桃園市儀器商業同業公會、臺中市儀器商業同業公會、台南市儀器商業同業公會、高雄市儀器商業同業公會、新竹市儀器商業同業公會、台灣橡膠暨彈性體工業同業公

會、台灣省橡膠製品商業同業公會聯合會、台北市國際工商協會、台灣生物產業發展協會、台灣先進醫療科技發展協會、台北市美國商會政府及公共事務部、歐洲在臺商務協會、台北市日本工商會、南港軟體工業園區二期管理委員會、財團法人金屬工業研究發展中心(高雄)、財團法人台灣商品檢測驗證中心、社團法人中華無菌製劑協會、台灣省進出口商業同業公會聯合會、新北市進出口商業同業公會、桃園市進出口商業同業公會、台中市進出口商業同業公會、台中縣進出口商業同業公會、台南市進出口商業同業公會、台南縣進出口商業同業公會、高雄縣進出口商業同業公會、高雄市進出口商業同業公會、台灣臨床檢驗標準協會、台灣製藥工業同業公會、中華民國西藥商業同業公會全國聯合會、台灣省西藥商業同業公會聯合會、中華生物醫學工程協進會、中華民國金屬家具商業同業公會全國聯合會、中華民國生物醫學工程學會、台灣顯示器產業聯合總會、新北市生技產業發展聯盟、台灣醫藥品法規學會、台灣科學工業園區科學工業同業公會、財團法人工業技術研究院量測技術發展中心、財團法人生物技術開發中心、台灣區電機電子工業同業公會、台灣藥物臨床研究協會、台北市西藥商業同業公會、中華民國開發性製藥研究協會、中華民國製藥發展協會、台北市電腦商業同業公會、中華民國全國商業總會、中華民國全國工業總會、台灣研發型生技新藥發展協會、經濟部工業局、科技部新竹科學園區管理局、科技部南部科學園區管理局、科技部中部科學園區管理局、財團法人塑膠工業技術發展中心、財團法人醫藥品查驗中心、財團法人醫藥工業技術發展中心、台北市進出口商業同業公會、中華民國西藥代理商業同業公會、台北市西藥代理商業同業公會、台灣藥品行銷暨管理協會、中華民國資訊軟體協會

副本：

署長吳秀梅

裝 訂 線

正本

檔　　號：
保存年限：

衛生福利部食品藥物管理署　公告

發文日期：中華民國110年5月3日
發文字號：FDA器字第1101603391號
附件：適用於製造業者之醫療器材網路安全指引1份

主旨：公告「適用於製造業者之醫療器材網路安全指引」

依據：行政程序法165條

公告事項：

一、公告「適用於製造業者之醫療器材網路安全指引」(如附件)，以提供廠商做為產品研發及申請查驗登記資料準備之參考。

二、本案另載於本署全球資訊網站(www.fda.gov.tw)之公告區及及醫療器材法規專區。

三、本署108年11 月18 日FDA器字第1081600444號公告自即日起停止適用。

署長 吳秀梅

適用於製造業者之醫療器材網路安全指引

110.05.01版

一、前言

醫療器材網路安全(Cybersecurity)，是針對醫療器材因網路行為或資料傳輸引起的安全問題，防止醫療器材被未經授權的存取、修改、誤用或拒用，使功能減損而導致病患傷害， 或避免資訊係經由醫療器材被未經授權的存取或轉移至外部接受者。

為利製造業者確保醫療器材之網路安全，爰制訂「適用於製造業者之醫療器材網路安全指引」。本指引提出製造業者於產品設計、研發、申請查驗登記及產品核准上市後應考量之網路安全相關事宜。本指引為行政指導文件，各界可自行參酌運用。

本指引內容為中央主管機關依據現行之參考資料擬定，惟科技發展日新月異，法規更新未逮之處，為確保國人健康安全，審查人員可能視產品軟體架構與設計之技術特點，要求廠商提供本指引所列項目外之網路安全驗證評估資料；另本指引將不定期更新。

本指引所引用之相關國際標準或指引若有更新版本，廠商得自行引用更新版本。另若有其他醫療器材網路安全相關國際標準，廠商亦得自行參考引用。

二、名詞定義

（一）、**網路安全(Cybersecurity)-** 防止醫療器材被未經授權的存取、修改、誤用或拒用， 或避免資訊係經由醫療器材被未經授權的存取或轉移至外部接受者的過程。

（二）、**機密性(Confidentiality)-** 資料、資訊及系統架構僅可由被授權之人員與實體機構存取使用，並且在授權時間點與授權方式下進行處理，以確保資料與系統安全性。機密性確保無未獲授權之使用者(如:只有被信任的使用者)可存取資料、資訊或系統架構。

（三）、**完整性(Integrity)-** 資料、資訊、軟體、系統維持其準確與完整，且未受不當修改。

（四）、**可取得性(Availability)-** 資料、資訊、資訊系統，在預期方式下可及時存取與使用。

（五）、**傷害(Harm)-** 對人體實體的傷害或健康損傷(包括死亡)、對資產或環境的損害。

（六）、**身份驗證(Authentication)-** 確認使用者身分、操作程序或裝置之動作，作為允許存取使用醫療器材裝置、資料、資訊或系統之前置要件。

（七）、**授權(Authorization)-** 允許存取使用醫療器材裝置的權力或許可。

（八）、**威脅(Threat)-** 經由未授權的存取行為、資訊的破壞、揭露、修改，或阻斷服務(Denial of Service)，而可能導致器材、組織營運(包括組織任務、功能、形象、聲譽)、組織資產、個人、其他組織受到不良影響的情況或事件。

（九）、**漏洞(Vulnerability)-** 可能被威脅來源(Threat Source)利用的資訊系統、系統安全步驟、內部管控、人員行為上的弱點。

（十）、**威脅建模(Threat Modeling)-** 藉由識別潛在攻擊目標與漏洞來優化網路、應用程式及網路安全的方法，用於定義可防止或消除系統威脅的對策。對於醫療器材而言，威脅建模可用於識別出特定產品、特定產品線、組織供應鏈中可能導致患者傷害的漏洞與威脅，提升醫療器材的網路安全性。

（十一）、**補償性控制(Compensating Control)-** 製造業者用來替代或補充產品內建安全設計而採取的額外措施。這類控制不屬於原先設計的一部分，可於使用環境配置或可由使用者設置，以提供醫療器材補充性或同等性的網路保護。

（十二）、**可控風險(Controlled Risk)-** 因網路安全漏洞導致病患遭受傷害的殘餘風險低至可被接受者，則稱此類風險為可控風險。

（十三）、**未受控風險(Uncontrolled Risk)-** 出現的網路安全風險依現存之風險減輕措施及補償性控制仍無法讓病患遭受傷害的殘餘風險降至可被接受者，則稱此類風險為未受控風險。

（十四）、**例行性網路安全更新與修補(Cybersecurity Routine Updates and Patches)-** 強化醫療器材，用來提升醫療器材安全性並/或修正可能造成病患傷害的受控風險(Controlled Risk)漏洞，這類改變並非用於降低病患之未受控風險(Uncontrolled Risk)。包含任何用於提升醫療器材安全性之定期排程安全更新或修補，包括軟體、韌體、可程式邏輯、硬體、器材安全更新，以及早於定期排程預定週期所執行並用於處理與受控風險相關之更新與修補。例行性網路安全更新與修補通常會被視為一種加強醫療器材安全之方式，可

應用於與受控風險相關的安全漏洞，但並非被視為一種修復。但應注意，用於去除/修補使用產品可能會導致嚴重健康不良後果或死亡的相關重大安全更新，則不屬於例行性網路安全更新與修補。

（十五）、 **網路安全訊號(Cybersecurity Signal)-** 網路安全訊號是任何表現出網路安全可能或已確定發生網路安全漏洞的資訊，這種漏洞可使醫療器材受到影響。網路安全訊號可源自於傳統的訊息來源，例如內部調查、上市後監督、申訴，與/或以安全為導向的消息來源，例如電腦/網路緊急事件回應/ 準備小組(Computer/Cyber, Emergency Response/ Readiness Teams， 簡稱CERT)、威脅指標、安全研究人員。網路安全訊號可從醫療與公共衛生關鍵基礎設施內進行辨識，不過即使源自於其他關鍵基礎設施(例如國防、財政)的訊號，也可能影響醫療器材的網路安全。

（十六）、 **可利用的已知漏洞(exploit)-** 可利用的已知漏洞是一種安全威脅(意外或蓄意)造成一或多項漏洞的情況，不僅可能影響醫療器材的安全或基本必要效能，也可能將醫療器材作為載體，損害與其連線之器材或系統。

三、適用範圍

（一）、本指引適用於製造或研發任何與網路安全相關醫療器材之製造業者，包含但不限於：

1. 醫療器材產品其組成包含軟體(含韌體)或具有可程式邏輯裝置(Programmable Logic)者。
2. 醫療器材軟體(包括行動應用程式)。

（二）、本指引不適用於醫療機構及醫療器材操作人員、維護人員、資訊系統管理及整合者等之網路安全措施。

備註：軟體若依衛生福利部食品藥物管理署「醫用軟體分類分級參考指引」之判定參考原則，判定未列屬於醫療器材管理，則該軟體不屬於本指引適用範圍，例如醫院行政管理軟體、一般健康管理軟體、及用藥紀錄軟體等，有關醫療機構之資通安全建議參考資通安全管理法和資通安全管理法施行細則。

四、基本原則

（一）、為確保醫療器材能維持其安全與有效性，醫療器材製造業者應有一套網路安全管制措施，以確保醫療器材的網路安全，並應定期評估網路安全風險，以及依據風險評估結果，採取適當安全管理機制。網路安全管理計畫應同時涵蓋上市前及上市後階段，從產品設計開始直到產品結束生命週期。

（二）、醫療器材的網路安全維護係屬於各關係者，包含醫療器材製造業者、醫療器材使用者、醫療器材維護者、醫療機構、資訊系統管理者、資訊系統整合業者、健康醫療資訊開發業者以及資料軟體販售業者等各種關係人的共同責任。

（三）、為防止未經授權的存取、修改、誤用或拒用導致病患傷害，或是避免機密資料被未經授權的儲存、存取或轉移至外部接受者，醫療器材應維護其機密性(Confidentiality)和完整性(Integrity)，確保醫療器材軟體和資料的準確和完整，不會遭受不當修改而導致病患安全風險；同時醫療器材亦應具備可取得性(Availability)，使其產品功能不會因網路安全問題而減損，與資料能在預期方式下被及時存取與使用。

（四）、製造業者應將網路安全相關考量納入醫療器材設計輸入(Design Input)的一部分，並建立網路安全管理方法與措施，作為軟體確效及風險分析的一部分。這些分析須包含下列因素:

1. 辨識資產(Asset)、威脅及漏洞
2. 評估威脅及漏洞對醫療器材功能性及最終使用者(End User)、病患之影響性
3. 評估威脅及漏洞發生或被攻擊的可能性
4. 定義風險層級及適當的風險降低措施
5. 評估殘餘風險及風險可接受條件

（五）、醫療器材產品應針對網路安全威脅設計具備識別(Identify)、保護(Protect)、偵測(Detect)、回應(Respond)、復原(Recover)之相關網路安全核心功能架構。製造業者在面對網路安全威脅時，不論是上市前開發或上市後管理，皆應事先制定網路安全相關處理程序。

（六）、 製造業者思考如何完備醫療器材產品網路安全特性時，可參考國際相關評估指標。資訊安全要求和資訊安全風險管制措施之建議參考來源包括AAMI TIR57、IEC TR 80001-2-2、IEC TR 80001-2-8、ISO 27000系列、ANSI UL 2900系列、美國NIST (National Institute of Standards and Technology)、OWASP (Open Web Application Security Project)、ENISA(European Union Agency for Cybersecurity)以及美國醫療保健和公共衛生部門協調委員會聯合網路安全工作組(US Healthcare and Public Health Sector Coordinating Council (HPH SCC) Joint Cyber Security Working Group (JCWG))等。

（七）、表一列舉醫療器材製造業者在設計其產品之資訊安全時應考慮的之設計原則。

表一、網路安全設計原則

設計原則	描述
安全的通訊(Secure Communications)	製造業者應考慮器材如何與其他器材或網路連接。連接介面(Interface)可能包括實體連線(Hardwired Connections)和/或無線通訊，連接方式例如 Wi-Fi、乙太網路(Ethernet)、藍牙和 USB 等。
	製造業者應確認所有輸入(不僅是外部輸入)的設計特性，並考量不安全的器材和環境(例如，連接到家庭網路的器材或舊式器材)。
	製造業者應考慮如何確保器材間的資料傳輸安全，以防止未經授權的存取(Access)、修改(Modification)或重播(Replay)。例如，製造業者應確定器材/系統之間的通訊如何相互認證(Authenticate)、是否需要加密(Encryption)、如何防止先前發送的命令或資料被未經授權的重播、以及在預定時間後終止通訊是否合適。
資料的保護(Data Protection)	製造業者對於個人資料之蒐集、處理及利用須符合我國《個人資料保護法》、《個人資料保護法施行細則》等相關法規要求，善盡保護資料之職責。
	當製造業者跨國傳輸個人資料或將作業委託他人處理涉及使用雲端服務時須符合我國《個人資料保護法》等相關法規要求。

	製造業者應考慮對儲存在器材上或從器材傳輸的安全相關資料實施保護措施，例如加密(Encryption)，密碼應儲存爲加密的安全雜湊(Cryptographically Secure Hashes)。
	製造業者應考慮採取風險管制措施以保護通訊協議中的訊息控制/排序欄位(Message Control /Sequencing Fields)或防止密鑰資訊(Cryptographic Keying Materials) 受損。
資料的完整性(Data Integrity)	製造業者應評估系統層面的架構，以設計確保資料的不可否認性(Non-Repudiation)的功能(例如，支援稽核日誌的功能)。
	製造業者應考慮損害器材完整性的風險，例如未經授權就對器材軟體進行修改。
	製造業者應考慮管制措施(例如使用反惡意軟體(Anti-malware))，以防止病毒、間諜軟體(Spyware)、勒索軟體(Ransomware)以及其他形式的惡意程式碼(Malicious Code)在器材上執行的。
使用者身份驗證(User Authentication)	製造業者應考慮使用者存取管制(Access Controls)，以確認(Validate)誰可以使用該器材或允許向不同角色的使用者授予特權，或在緊急情況下允許使用者存取，並留下紀錄。此外，不應在器材和客戶之間共享相同的憑據(Credentials)。身份驗證或存取授權的例子包括密碼(Passwords)、硬體金鑰(Hardware Keys) 、軟體金鑰(Software Keys)或生物特徵(Biometrics) ，或其他器材無法產生的訊號。
軟體維護(Software Maintenance)	製造業者應建立定期(Regular)更新的流程。
	製造業者應考慮如何更新或管制作業系統軟體(Operating System Software)、第三方軟體(Third-party Software)或開源軟體(Open Source Software)。製造業者還應規劃如何回應超出其管制範圍的軟體更新或過時的作業環境(例如，在不安全的作業系統版本上運行的醫療器材軟體)。
	製造業者應考慮如何更新器材，使其不受新發現的網路安全漏洞影響。例如，可以考慮更新是否需要使用者介入或由器材啟動，以及

	如何確認更新，以確保更新不會對器材的安全和功效產生不利的影響。
	製造業者應考慮使用程式碼簽章(Code Signing)或其他類似方法進行更新所需的連接，以及連接或更新的真實性(Authenticity)。
實體存取(Physical Access)	製造業者應考慮採取管制措施，以防止未經授權的人員存取器材。例如，管制可能包括實體鎖或在實體上限制對埠(Port)的存取，或者不允許使用不需要身份驗證的實體電纜(Physical Cable)進行存取。
可靠性(Reliability)和可取得性(Availability)	製造業者應考慮設計使器材能夠偵測(Detect)、抵抗(Resist)、回應(Respond)並從網路安全攻擊中復原(Recover)的功能，以保持其基本功效。

五、網路安全風險管理原則

（一）、醫療器材製造業者應於醫療器材生命週期間，持續建立、記錄及進行下列流程，包含識別與醫療器材網路安全相關的危害、預測與評估相關風險、執行風險控制、以及監控各項控制措施之成效；在進行上述流程時，應涵蓋風險分析、風險評估、風險管制、產品生產前後的資訊整合等程序。應分析之項目如下:

1. 維持安全與主要效能
2. 網路安全訊號(Cybersecurity Signals)識別
3. 漏洞特徵分析與評估
4. 風險分析與威脅建模
5. 威脅來源分析
6. 產品威脅偵測能力整合
7. 所有產品之影響評估
8. 補償性控制評估

9. 風險減輕措施與殘餘風險評估

（二）、醫療器材製造業者應針對產品安全風險(Safety Risk)和網路安全風險(Cybersecurity Risk)皆制訂有風險分析與管理機制，當其中一種風險管理機制，基於對特定風險的分析結果，而決定將特定安全措施新增至產品設計時，必須同時將此安全措施導入另一種風險管理機制進行評估，惟有在兩種風險評估報告中，都能將殘餘風險降低至可接受程度後，該安全措施才能被設計執行。

（三）、醫療器材製造業者應於執行網路安全風險分析前，事先擬定一套「網路安全風險管理計畫」，於計畫中應針對下列內容進行明確定義:

1. 風險分析與評估方法
2. 可接受殘餘風險的鑑別
3. 風險確效的方法
4. 產品上市後的網路安全監控機制
5. 網路安全訊息的收集方式
6. 已識別網路威脅和漏洞的定期檢視
7. 已識別安全漏洞的揭露政策
8. 安全有效性相關的軟體更新程序

（四）、執行網路安全風險分析時，應先定義出醫療器材與網路安全有關的預期用途和功能特徵，同時亦必須識別出可能遭遇的威脅、漏洞、需保護的資產以及可能的負面影響等；製造業者應依產品特性選擇適當的分析方法，例如威脅建模等，藉以識別出產品中可能導致傷害的漏洞與威脅，進而提升醫療器材的安全性。

（五）、製造業者應執行一套定義明確的流程，採用系統化方式執行風險評估，藉以判斷醫療器材的網路安全漏洞風險是否可接受，製造業者應評估流程詳細定

義與文件化， 以佐證其網路安全風險評估之客觀性。風險評估流程應同時考慮網路安全漏洞遭利用之可能性(Exploitability)，以及造成的病患傷害嚴重度(Severity)。製造業者進行分析時，亦應將補償性控制與風險減輕措施納入考量。

（六）、製造業者評估網路安全漏洞可能造成的可利用的已知漏洞嚴重度時，應考慮採用客觀性的網路安全漏洞評估工具，或使用類似的漏洞評分系統來判斷應變的需求與緊急程度，例如通用漏洞評分系統(Common Vulnerability Scoring System, CVSS)、通用漏洞揭露資料庫(Common Vulnerabilities and Exposures, CVE)等。在評估的過程中，應納入不同考量因素，並給予不同等級之數值評分，如下列參考範例:

- 攻擊向量(實體、本地、鄰近、遠端網路)
- 攻擊複雜度(高、低)
- 權限需求(無、低、高)
- 使用者互動(不需要、需要)
- 範圍(有變化、無變化)
- 機密性影響(高、低、無)
- 完整性影響(無、低、高)
- 可取得性影響(高、低、無)
- 可利用的已知漏洞代碼成熟度(高、功能性、概念驗證、未經驗證)
- 修正級別(無可用修補、權宜措施、臨時性修補、製造業者官方修補、未定義)
- 通報可信度(已證實、合理、未知、未定義)

（七）、如網路安全漏洞可能遭人利用，製造業者應設置病患傷害嚴重度的評估流程，執行此類分析有諸多可行方式，例如可參考ISO 14971 所提之定性化(qualitative)傷害嚴重度分級:

常見用詞	可能的描述
可忽略:	不方便或暫時性的不適

輕微:　　暫時性損傷，不需專業醫療介入

嚴重:　　造成需要專業醫療介入的損傷

危險:　　造成永久性或具生命威脅性的損傷

致命:　　造成患者死亡

（八）、執行網路漏洞風險評估的主要目的在於檢視病患傷害風險是否受到控制(可接受程度)或未受控制(不可接受程度)。建議可使用「漏洞遭利用之可能性」與「傷害嚴重度」組合的矩陣，藉以描繪出「漏洞遭利用之可能性」與「傷害嚴重度」之間的關係，可用於評估網路安全漏洞導致的傷害風險程度，並作為「可控風險」或「未受控風險」之評估工具，如下列參考範例:

漏洞遭利用導致的傷害嚴重度 (Seventy of Patient Harm (if exploited))

漏洞遭利用之可能性 (exploitability)	可忽略 (Negligible)	輕微 (Minor)	嚴重 (Serious)	危險 (Critical)	致命 (Catastrophic)
高(High)					
中(Medium)					
低(Low)					

六、 網路安全測試項目

所有網路安全的風險管制措施皆應根據設計規格和/或設計需求進行查證和確認。關於網路安全的測試，建議參考本指引四、(六)等相關國際標準。

製造業者應針對醫療器材網路安全機制進行適當的確效測試，例如對程式碼進行惡意軟體測試(Malware Testing) 以確保軟體不會潛藏已知的危害風險；透過外部界面輸入資料進行異常輸入測試(Malformed Input Testing)，驗證產品在隨意或意外輸入的情況下，能維持其正確運作；亦可考慮實施結構性滲透測試(Structured Penetration Testing)，嘗試規避風險管控措施和安全維護組態，入侵服務系統、設備等產品相關軟硬體，找出各種潛在的漏洞，藉以驗證產品的資料與功能是否可被竊取或破壞，評估軟體系統與硬體安全性是否有待加強。

表二列舉製造業者在查證和確認過程中可能考慮的測試類型。

表二、可能考慮的網路安全測試項目

測試類別	測試說明
漏洞和可利用的已知漏洞測試 (Vulnerabilities and Exploits Testing)	已知漏洞測試：針對已知的漏洞資料庫(例如，美國國家漏洞資料庫(National Vulnerability Database))測試軟體程式。
	惡意軟體測試：用惡意軟體檢測工具掃描程式以確定是否存在任何已知的惡意軟體。
	異常輸入測試(Malformed Input Testing、即模糊測試 FUZZ Testing)：器材遭受到大量的異常輸入(無效或非預期的輸入)，以觀察器材是否會以非正常的方式運行或是否“當機(Crash)”。
	結構化的滲透測試(Structured Penetration Testing)：這種類型的測試需要熟悉駭客技術(例如，白帽(White Hat)或道德駭客(Ethical Hacker))的網路安全專家，網路安全專家會以試圖繞過器材設計的防禦層之方式進行測試。
軟體弱點測試 (Software Weakness Testing)	靜態原始碼分析(Static Source Code Analysis)：無需執行軟體程式，利用軟體工具來檢查原始碼有無存有程式邏輯或安全設計缺陷等可能衍生後續安全上的問題。
	靜態二進位碼與位元組碼分析(Static Binary and Bytecode Analysis)：使用軟體工具進行分析與反組譯，檢查有無存有程式邏輯或安全設計缺陷等可能衍生後續安全上的問題。

七、 上市前審查要求

醫療器材製造業者應明確記錄與網路安全相關的活動，於查驗登記申請時提交網路安全相關文件，說明如表三。

表三、網路安全相關上市前審查要求

上市前審查資料	說明
設計文件(Design Documentation)	包括任何界面(Interfaces)、通訊途徑、元件(硬體和軟體)，以及為緩解與患者傷害有關的網路安全風險的所有設計功能，如存取管制(Access Control)、加密、安全更新、日誌紀錄、實體安全(Physical Security)等。 請參考本指引四、基本原則。
風險管理文件(Risk Management Documentation)	描述網路安全威脅和漏洞、相關風險的評估、爲緩解這些風險而採取的管制措施的描述、以及證明這些管制措施已經過充分測試的證據。製造業者應考慮可讓器材網路安全最大化且不過度影響其他安全的管制措施，建議參考網路安全風險管理標準(例如 AAMI TIR57：2016，AAMI TIR97：2019)以及 ISO 14971：2019 等。風險管理文件包含內容如下: ● 全面的風險管理文件，例如風險管理報告或資訊安全風險管理報告，該報告應包括威脅建模(Threat Modeling)、可識別的網路安全威脅及其供應商(例如雲端、晶片、軟體等)進行資訊安全風險評估。 ● 資訊安全風險緩解措施對其他風險管理的影響之探討。
資訊安全測試文件(Security Testing Documentation)	爲查證器材的資訊安全和緩解措施的有效性而進行的所有測試之測試報告。 網路安全相關測試資料應包括檢驗規格(含各測試項目之合格範圍及其制定依據)、方法、原始檢驗紀錄及檢驗成績書。

	請參考本指引六、網路安全測試項目。
追溯性矩陣(Traceability Matrix)	連結資訊安全風險、資訊安全管制措施和測試之追溯性矩陣(Traceability Matrix)。
軟體物料清單(Software Bill of Material, SBOM)	SBOM 包括但不限於開源和現成(Off-the-shelf)軟體元件(Components)之清單，該清單透過名稱、來源、版本(Version)和內部版本(Build)來識別每個軟體元件，以使器材使用者(包括病患和醫療保健提供者)能夠有效地管理其資產，了解已識別的漏洞對器材(和連接的系統)的潛在影響，並部署對策以維護器材的安全和功效。
說明書及相關文件(Labelling and Documentation)	說明書建議包含下列內容: ● 醫療器材製造業者、醫療器材使用者(含醫療機構)、資訊系統整合業者、健康醫療資訊開發業者以及資料軟體販售業者等各種關係人對於個人資料之蒐集、處理和利用須符合我國《個人資料保護法》要求。 ● 預期使用環境下的網路安全建議，例如反惡意軟體、網路連接組態(Configuration)、防火牆的使用等。 ● 預期接收和/或發送資料的網路埠(Network Ports)和介面(Interfaces)的清單，以及埠功能的描述(說明埠是傳入還是傳出，未使用的埠應要禁用(Disabled))。 另建議下列相關文件: ● 有關備份和復原功能以及恢復組態的過程之說明。 ● 加密方式。 ● 呈現所有使用者需要了解的資訊之系統圖。

八、上市後網路安全監管

（一）、 製造業者應制定完善的上市後網路安全風險管理計畫與文件紀錄，包含但不限於申訴處理、品質稽核、矯正與預防措施、軟體確效與風險分析、售後服務等。

（二）、 網路安全管理計畫應包括網路安全資訊來源及第三方軟體元件的監控，以便於器材的總產品生命週期中找出新的漏洞；針對修正漏洞的軟體更新與修補制訂相關查證與確認程序，包括與市售軟體相關的更新與修補；持續了解、評估、偵測網路漏洞的存在與影響之程序；建立與使用者的溝通管道以收集網路危害訊息；採用風險分析模式，例如威脅建模等，以評估分析如何發展網路安全風險減輕管制措施來維持產品的安全性與效能； 採用共通性的網路安全危害訊息揭露政策與規範；儘早實施可於漏洞遭利用前改善網路安全風險的危害減輕措施。

九、危害處置與通報原則

（一）、 針對可能導致病患遭受傷害的殘餘風險低至可被接受之可控風險，製造業者即便在殘餘風險為可接受程度時，仍應積極維護及增進安全的網路環境，盡力降低網路安全風險。即便安全風險已受控制，亦鼓勵製造業者可採取其他控制程序，做為「深度防禦(Defense-in-depth)」策略的一環。

（二）、 關於處理與可控風險相關的安全漏洞事項之例行性網路安全更新與修補，這類變動被視為一種加強醫療器材安全的措施，不需提出申請，但應紀錄網路安全漏洞資訊與例行性網路安全更新與修補之詳細資訊，主管機關於必要時將視情況要求製造業者提供相關資料。

（三）、 當風險降低與補償性控制措施不足，可能產生病患遭受傷害的殘餘風險不可被接受之未受控風險。製造業者應盡速處理未受控風險。

由於漏洞修補方案未必可立即取得或實行，製造業者於發現安全漏洞之最短時間內(不超過 15 天)應通知給客戶及使用者，告知安全漏洞、識別並提供臨時的風險補償性控制措施，並制定計畫將殘餘風險降至可接受程度。風險管制措施必須確保不會對器材之安全及有效性造成更大的風險。醫療器材製造業者應將相關資訊文件

化並保存，包含矯正計畫的處理時間點及理論依據。製造業者對於顧客及使用者的通知應至少包含下列內容:

1. 敘明安全漏洞相關資訊，包含製造業者依據現有資訊推估可能對使用者造成的影響。
2. 說明製造業者為儘速降低病患傷害而進行中的措施。
3. 說明補償性控制措施(若適用)。
4. 說明製造業者正致力於修補安全漏洞或提供深度防禦策略，以降低發生傷害的機率與嚴重性，並且將於未來修補程式可使用時與客戶及使用者聯繫。

製造業者於得知漏洞後，應盡快修補安全漏洞，驗證修正處，並將修補程式提供給客戶及使用者，以便將殘餘風險降至可接受程度。在某些情況下，補償性控制措施可以做為一個降低殘餘風險至可接受程度的長期解決方案。補償性控制措施必須確保不會對器材之安全及有效性造成更大的風險。此外，製造業者於必要時應針對最終使用者進行追蹤。

（四）、 若未受控風險於國內導致嚴重不良反應，應於得知此類反應情形後，依「醫療器材嚴重不良事件通報辦法」，於規定之時限內向中央衛生主管機關或其委託機構通報。若製造業者評估未受控風險可能導致嚴重不良反應，則於得知此類風險存在情形後，不論是否已發生嚴重不良反應，參酌前開規定，向中央衛生主管機關或其委託機構通報未受控風險資訊及可能導致的嚴重不良反應。

（五）、 如發生適用個人資料保護法或其他法規規範之安全危害事件，製造業者除應遵循本指引前述醫療器材網路安全危害事件之處置及通報要求，亦應依相關法規規定事項辦理通報及其他必要處置。

（六）、 不論例行性/非例行性更新，若涉及規格或效能變更，應依「醫療器材管理法」及「醫療器材許可證核發與登錄及年度申報準則」相關規定辦理變更登記。

十、參考資料

1. 醫療器材管理法
2. 醫療器材許可證核發與登錄及年度申報準則

3. 個人資料保護法

4. 個人資料保護法施行細則

5. 資通安全管理法

6. 資通安全管理法施行細則

7. IMDRF: Principles and Practices for Medical Device Cybersecurity, 2020

8. US FDA: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices- Draft Guidance, 2018

9. US FDA: Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, 2005.

10. US FDA: Guidance for Industry and FDA Staff: Postmarket Management of Cybersecurity in Medical Device, 2016.

11. US FDA: Guidance for Industry and FDA Staff: Design Considerations and Premarket Submission Recommendations for Interoperable Medical Device, 2017.

12. US FDA: Guidance for Industry and FDA Staff: Deciding When to Submit a 510(k) for a Software Change to an Existing Device, 2017.

13. US FDA: Guidance for Industry and FDA Staff: Guidance for the Content of Premarket Submission for Software Contained in Medical Devices, 2005.

14. Health Canada: Guidance Document: Pre-market Requirements for Medical Device Cybersecurity, 2019

15. TGA: Medical device cyber security guidance for industry, 2019

16. Saudi Food and Drug Authority: Guidance to Pre-Market Cybersecurity of Medical Devices, 2019

17. ISO 14971:2019, Medical devices - Application of risk management to medical devices

18. IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities

19. IEC/TR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls.

20. IEC/TR 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

21. ISO/IEC 27000 family - Information security management systems

22. ANSI/AAMI TIR57:2016, Principles for medical device security-Risk management

23. AAMI TIR 97:2019, Principles for medical device security—Postmarket risk management for device manufacturers

24. ANSI UL 2900-1:2017, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

25. ANSI UL 2900-2-1:2017, Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems

26. HIMSS/NEMA Standard HN 1-2013, Manufacturer Disclosure Statement for Medical Device Security form (MDS2)

27. National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure Cybersecurity

28. National Institute of Standards and Technology (NIST): Guide for Conducting Risk Assessments, September 2012