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：黃琪惠02-27877554
電子郵件信箱：whitney@fda.gov.tw

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 108. 09. 06 文
檔號： 08559

發文日期：中華民國108年9月3日
發文字號：FDA器字第1081607792號
速別：普通件
密等及解密條件或保密期限：
附件：「適用於製造廠之醫療器材網路安全指引」草案

主旨：檢送「適用於製造廠之醫療器材網路安全指引」草案乙份，請轉知所屬會員，如有意見或修正建議者，請於108年9月30日前提供書面意見至本署，請查照。

說明：隨著資通訊科技及網路應用快速發展，可連接網路、無線傳輸式(Wireless)醫療器材越加普及，所衍生的網路行為或資料傳輸引起的醫療器材網路安全(Cybersecurity)亦備受挑戰，為利製造廠確保醫療器材之網路安全(Cybersecurity)，爰制訂「適用於製造廠之醫療器材網路安全指引」，以提供作為產品研發、申請查驗登記資料準備及產品核准上市後應考量之網路安全相關事宜之參考。

正本：台灣醫療暨生技器材工業同業公會、台灣先進醫療科技發展協會、新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、嘉義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、臺南市醫療器材商業同業公會、臺北市醫療器材商業同業公會、臺中市醫療器材商業同業公會、高雄市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、臺南市直轄市醫療器材商業同業公會、中華民國醫療器材商業同業公會全國聯合會、彰化縣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、桃園縣助聽器商業公會、台中市助聽器商業同業公會、高雄市助聽器商業同業公

會、彰化縣助聽器商業同業公會、中華民國行動輔具協會、台灣醫療照護輔具協會、中華民國儀器商業同業公會全國聯合會、嘉義市儀器商業同業公會、台北市儀器商業同業公會、臺中市儀器商業同業公會、臺北市儀器商業同業公會、高雄市儀器商業同業公會、桃園縣儀器商業同業公會、新竹市儀器商業同業公會、中華生物醫學工程商業協進會、台灣醫藥品法規學會、財團法人金屬工業研究發展中心(高雄)、財團法人金屬工業研究發展中心(台北)、財團法人塑膠工業技術發展中心、財團法人台灣電子檢驗中心、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、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、台灣生物產業發展協會、中華民國西藥商業同業公會全國聯合會、屏東縣醫療器材商業同業公會、中華民國金屬家具商業同業公會全國聯合會、台南市儀器商業同業公會、台北市國際工商協會、台灣醫療器材門市發展協會、中華民國全國商業總會、中華民國全國工業總會、台北市美國商會政府及公共事務部、歐洲在台商務協會、台北市日本工商會、台灣研發型生技新藥發展協會、南港軟體工業園區管理委員會、台灣科學工業園區科學工業同業公會、台灣省進出口商業同業公會聯合會、台北市進出口商業同業公會、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、台灣區電機電子工業同業公會

副本：

署長吳秀梅

1081607792

裝 訂 線

適用於製造廠之醫療器材網路安全指引(草案)

108.8

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。

為利製造廠確保醫療器材之網路安全(Cybersecurity)，爰制訂「適用於製造廠之醫療器材網路安全指引」。本指引提出製造廠於產品設計、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、背景說明

隨著資通訊科技及網路應用快速發展，可連接網路、無線傳輸式(Wireless)醫療器材、醫療用行動應用程式(Mobile Applications, APP)、運用智慧型通訊手機之醫療器材(Smartphone Based Devices)及雲端醫療應用也越加普及；產品所包含的軟體應用型態和傳遞之資訊內容更加複雜而多元，在不同醫療器材之間可能存在交互操作之控制連結，多項醫療器材亦可能透過網路連結，而構成複雜資訊系統的一部分。於此情況下，隨著使用無線傳輸、網際網路(Internet)及內網連接(intranet)技術的醫療器材日漸增加，醫療器材及醫療器材相關健康資訊(Medical Device-related Health Information)之電子資訊交換越加頻繁，如何有效的確保醫療器材之網路安全，以維護醫療器材的安全及效能為一重要考量。

隨著醫療器材所涉及的軟體及資訊系統的複雜化，醫療器材的網路安全已不能單獨依靠製造廠本身的維護措施來確保，包含使用者的操作習慣、設備的網路工作環境、資訊系統的連結等，都會影響到醫療器材的網路安全特性；另一方面，資訊技術的不斷進步，也

使網路攻擊的手法日新月異，任何系統都無法僅依賴特定的防護措施而能長期確保網路安全不受侵害。

因此，醫療器材的網路安全維護係屬於各關係者，包含醫療器材製造廠、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的共同責任。若無法維護醫療器材的網路安全，將可能造成醫療器材功能性減損、醫療機構或個人資料可取得性或完整性降低，甚至使其他連接裝置或內網系統受到安全威脅，進而可能導致患者傷害、死亡等事件發生。

醫療器材製造廠應有一系列網路安全控制措施，以確保醫療器材之資訊安全，並維持醫療器材之安全及有效性。本指引提出製造廠於產品設計、研發、申請查驗登記時以及產品上市後應考量之網路安全相關要點。其餘關係者(如醫療機構及醫療器材操作人員、資訊系統整合者等)之網路安全措施非屬本指引探討範圍。

三、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、數據資料、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)、 **脆弱性(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)、 **威脅模型(Threat Modeling)-** 藉由識別潛在攻擊目標與脆弱性來優化網路、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，威脅模型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，提升醫療器材的安全性。

(十一)、 **補償性控制(Compensating Control)-** 製造廠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)-** 因網路安全脆弱性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)脆弱性，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脆弱性，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脆弱性或異常行為的資訊，這種脆弱性或異常行為可

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)、 **異常行為(exploit)-** 異常行為是一種安全威脅(意外或蓄意)造成一或多項脆弱性的情況，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。

四、適用範圍

(一)、本指引適用於製造或研發任何可建立連結醫療器材之製造廠，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、資訊系統整合者等之網路安全措施。

備註：依衛生福利部 104 年 4 月 13 日發布之「醫用軟體分類分級參考指引」，醫療器材軟體可能存在之形式如下:

1. 醫療器材的附件: 電子醫療器材本身內建的軟體，或為該器材的附屬物，包含安裝在電腦介面以驅動、控制醫療器材的軟體。
2. 單獨的軟體(Stand-alone Software): 這類醫療器材軟體或應用程式並不是醫療器材的一部分，通常會和器材分開上市，可以處理、分析醫療儀器產生的資料，協助診斷、治療用途。
3. 行動應用程式(Mobile Applications): 這類軟體可安裝在行動電話、平板電腦或其他電子產品上，可能搭配醫療器材使用，此類應用程式若用於醫療目的，並依「醫用軟體分類分級參考指引」判定屬醫療器材列管，則應符合醫療器材軟體之規定。

4. 儲存軟體的紀錄媒體(Record Media): 醫療器材軟體可以儲存於光碟、記憶卡（SD）、隨身碟等實體記錄媒體，或可經由網路伺服器線上下載，無論軟體以何種形式供應，只要符合醫療器材定義，皆需符合醫療器材相關規定。
5. 前述軟體若依「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。

五、基本原則

(一)、 為確保醫療器材能維持其安全與有效性，醫療器材製造廠應有一套網路安全控制措施，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，包含醫療器材製造廠、醫療器材使用者、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，或是避免機密數據被未經授權的儲存、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數據的準確和完整，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，與數據能在預期方式下被及時存取與使用。

(四)、 製造廠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)、威脅及脆弱性
2. 評估威脅及脆弱性對醫療器材功能性及最終使用者(End User)、病患之影響性
3. 評估威脅及脆弱性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、保護、偵測、應變、回復之相關網路安全核心功能架構。製造廠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)、 醫療器材產品進行上市前審查時，製造廠應提交符合上述網路安全管理要求之佐證資料；當產品上市後發生嚴重藥物不良反應時，須依「嚴重藥物不良反應通報辦法」規定，向中央衛生主管機關或其委託機構通報危害情形及所採取的相關補救措施，以確認產品所遭受之危害風險，經適當處置後已降至可接受的程度。

六、網路安全風險管理原則

(一)、 醫療器材製造廠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、風險控制、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. 脆弱性特徵分析與評估
4. 風險分析與威脅模型
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)、 醫療器材製造廠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)、 醫療器材製造廠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. 已識別網路威脅和脆弱性的定期檢視；
7. 已識別安全脆弱性的揭露政策；
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、脆弱性、需保護的資產以及可能的負面影響等；製造廠應依產品特性選擇適當的分析方法，例如威脅模型等，藉以識別出產品中可能導致傷害的脆弱性與威脅，進而提升醫療器材的安全性。

(五)、 製造廠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脆弱性風險是否可接受，製造廠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脆弱性的異常行為嚴重度(Exploitability)，以及造成的病患傷害嚴重度(Severity)。製造廠進行分析時，亦應將補償性控制與風險減輕措施納入考量。

(六)、 製造廠評估網路安全脆弱性的異常行為嚴重度時，應考慮採用客觀性的網路安全脆弱性評估工具，或使用類似的脆弱性評分系統來判斷應變的需求與緊急程度，例如通用脆弱性評分系統(Common Vulnerability Scoring System, CVSS)、通用脆弱性披露資料庫(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:

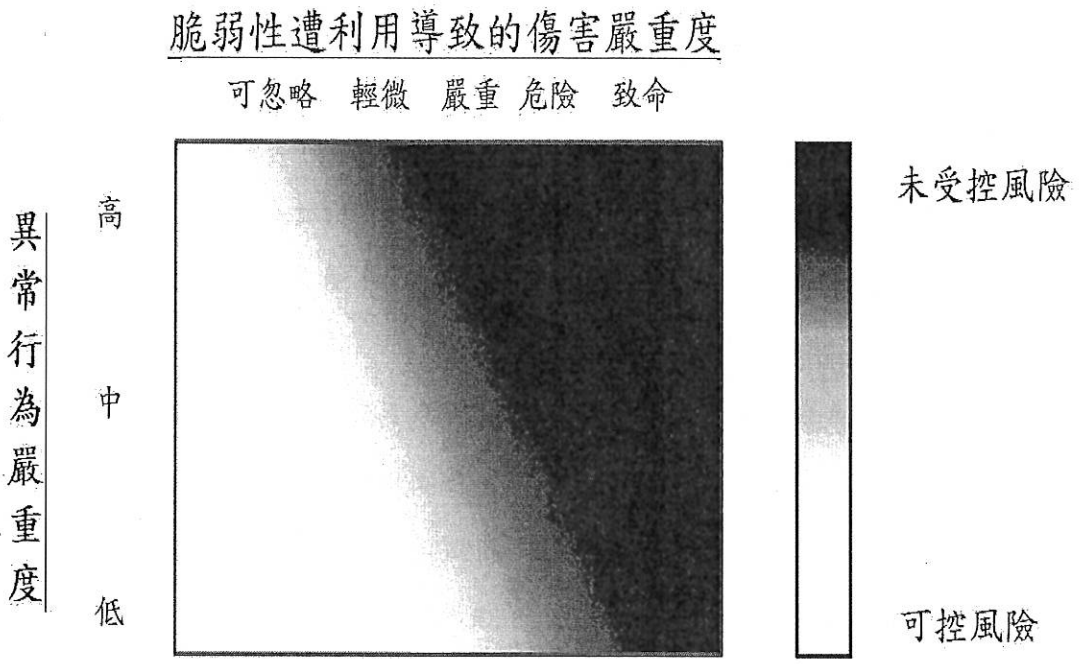
- 攻擊向量（實體、本地、鄰近、遠端網路）
- 攻擊複雜度（高、低）
- 權限需求（無、低、高）
- 使用者互動（不需要、需要）

- 範圍（有變化、無變化）
- 機密性影響（高、低、無）
- 完整性影響（無、低、高）
- 可用性影響（高、低、無）
- 異常行為代碼成熟度（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、製造廠官方修補、未定義）
- 通報可信度（已證實、合理、未知、未定義）

(七)、如網路安全脆弱性可能遭人利用，製造廠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 所提之質性傷害嚴重度分級:

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)、執行網路脆弱性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「異常行為嚴重度」與「傷害嚴重度」組合的矩陣，藉以描繪出「異常行為嚴重度」與「傷害嚴重度」之間的關係，可用於評估網路安全脆弱性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:



七、網路安全功能

製造廠對其製造之醫療器材產品應針對網路安全威脅設計具備識別、保護、偵測、應變、回復之相關網路安全核心功能架構。

(一)、 識別及保護(Identify and Protect)

具有連結(以無線或實體線路連接)至其他醫療器材、網際網路、其他內網或可攜式儲存設備(如 USB 或 CD)之醫療器材，相較於無相關連接功能者，較可能暴露於網路資訊安全威脅，這時就須要進行網路安全控制。網路安全控制的方式需考量器材之預期用途、預期之電子資料介面、預期使用環境、網路安全脆弱性形式、網路安全脆弱性發生率及病患可能之傷害。

醫療器材製造廠應審慎考量如何在網路安全保障及預期使用環境下的醫療器材可用性(Usability)達成平衡，以確保醫療器材中的安全控制適用於預期使用者。例如，若無合理理由，安全控制不應妨礙醫療器材於預期用途範圍內適用於緊急情況下的使用。

醫療器材製造廠於上市前申請審查時，應於送審文件說明其醫療器材產品使用之網路安全功能(Cybersecurity Functions)。保護醫療器材之網路安全功能包含，但不限於下列項目:

1. 限制僅有經授權的可信賴使用者才能進行存取使用(Limited Access to Trusted Users Only):

(1)、醫療器材應設計具備身分驗證機制來限制裝置存取，例如用戶帳號與密碼、智慧卡(Smartcard)、生物辨識科技(Biometric Technology)。

(2)、根據使用者角色（例如照護者、系統管理員）或裝置角色實施分級授權模式(Layered Authorization Model)。

(3)、採用適當身份驗證方式以設定不同權限。(例如透過多重驗證方法為系統管理人員、服務技術人員、維護人員等不同人員設置裝置存取權限)。

(4)、醫療器材應具備防範未經授權使用之相關功能特性，例如使用自動計時方式終止系統使用（視適用情況實施)、強化密碼保護機制並定期更新、採用裝置與通訊埠的實體鎖以降低密碼竄改機會、在同意軟體或韌體更新以前（包括作業系統、應用程式、防惡意軟體的更新)，要求身分驗證或其他適當控制程序等。

2. 確保可信賴的內容(Ensure Trusted Content):

(1)、醫療器材執行軟體或韌體更新時，應確保為經驗證之程式碼，製造廠應考慮軟體或韌體更新須採用適當的認證機制，例如驗證碼(Authenticated Code)、代碼簽名認證（Code Signature Verification）等方式，並應採用系統化程序，供授權用戶於廠商端下載可識別版本之軟體與韌體。

(2)、針對敏感性資料的儲存及傳輸於可行時進行加密保護機制。

(二)、偵測、應變、回復(Detect, Respond, Recover)

1. 醫療器材應具備相關功能特性，使產品在正常使用下能夠偵測(Detected)、辨識(Recognized)、記錄(Logged)、時間控制(Timed)、處理(Acted)網路安全功能減損之情形。

2. 針對醫療器材之關鍵功能，則應設計實施相關保護措施，即便產品的網路安全已受減損，仍可保護產品不影響其關鍵功能。

3. 醫療器材亦應具備系統保存(Retention)及回復(Recovery)功能，可以提供通過驗證之特定授權人員，維持與復原產品組態的方法。

4. 應針對最終使用者提供當偵測到資訊安全事件時應採取的適當措施相關資訊。

(三)、 製造廠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，例如 IEC 80001-2-2:2012 標準及 HIMSS/NEMA Standard HN 1-2013《醫療器材網路安全特性製造廠聲明表格》 (Manufacturer Disclosure Statement for Medical Device Security form, MDS^2 form)，針對自動登出、稽核控管、授權機制、安全特徵組態、網路安全更新、健康資料去識別化、數據備援、緊急使用、醫療數據的完整性與正確性、惡意軟體偵測與防護、網路節點識別、使用者識別、器材硬體鎖、第三方軟體控管、系統與應用程式韌性、安全性指引、資料儲存機密性、資料傳輸機密性、資料傳輸完整性等網路安全防護面向，依產品特性與預期用途進行自我評估，製造廠選擇產品適用之安全防護措施時，應有相關之文件紀錄以說明其合理性。

(四)、 製造廠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，找出各種潛在的脆弱性，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。

(五)、 醫療器材產品申請上市時，製造廠應提供下列醫療器材網路安全相關資料：

1. 產品敘述與說明資料，應包含以下內容:
    - 產品所有設計功能、安全維護功能及管理功能的描述；
    - 所有外部界面或實體輸入/輸出界面清單，包括遠端界面、本機界面、無線傳輸界面、外部檔案輸入，以及所有支援這些界面的通訊協定；
    - 所有可執行程式及函式庫清單、相關軟體建置和安裝整合程序之說明；
    - 產品生命週期內如何維持其網路安全的方法，以及如何提供經確效之軟體更新與修補程式之計畫；
    - 產品使用說明與產品規格等，包含預期使用環境下建議採用之網路安全控制方式:如網路安全組態和使用環境需求、能夠確保安全功能

有效性的操作說明、身份識別和授權的方法、防毒軟體及防火牆的使用等。

2. 產品設計與驗證資料，應包含因應意圖(Intentional)或非意圖(Unintentional)的網路安全風險之風險分析、風險管控措施、設計考量，以及說明每個風險管控措施如何實施，其中應包括；

- 產品設計過程中考量之網路安全風險清單；
- 產品建立之網路安全風險管控措施清單與理由說明；
- 連結網路安全風險分析及風險管控措施的可追溯矩陣圖；
- 簡要敘述用於確保醫療器材軟體之完整性(如防範惡意軟體)的控制措施；
- 各風險管控措施之確效資料

八、上市後網路安全監管

(一)、 製造廠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脆弱性；針對修正脆弱性的軟體更新與修補制訂相關驗證與確效程序，包括與市售軟體相關的更新與修補；持續了解、評估、偵測網路脆弱性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，例如威脅模型等，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；儘早實施可於脆弱性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，製造廠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，亦鼓勵製造廠可部署其他控制程序，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脆弱性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，但應將網路安全脆弱性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廠提供相關資料。

(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。製造廠應盡速處理未受控風險。

由於脆弱性修補方案未必可立即取得或實行，製造廠於發現安全脆弱性之最短時間內(不超過 15 天)應通知給客戶及使用者，告知安全脆弱性、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。醫療器材製造廠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。製造廠對於顧客及使用者的通知應至少包含下列內容:

1. 敘明安全脆弱性相關資訊，包含製造廠依據現有資訊推估可能對使用者造成的影響。
2. 說明製造廠為儘速降低病患傷害而進行中的措施。
3. 若有，說明補償性控制措施。
4. 說明製造廠正致力於修補安全脆弱性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顧客及使用者聯繫。

製造廠於得知脆弱性後，應盡快修補安全脆弱性，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，製造廠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「嚴重藥物不良反應通報辦法」，於規定之時限內向中央衛生主管機關或其委託機構通報。若製造廠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，製造廠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「藥事法」及「醫療器材查驗登記審查準則」相關規定辦理變更登記。

十、參考資料

1. US FDA: Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, 2005.
2. US FDA: Guidance for Industry and FDA Staff: Content of Premarket submissions for Management of Cybersecurity in Medical Devices, 2014.
3. US FDA: Guidance for Industry and FDA Staff: Postmarket Management of Cybersecurity in Medical Device, 2016.
4. US FDA: Guidance for Industry and FDA Staff: Design Considerations and Premarket Submission Recommendations for Interoperable Medical Device, 2017.
5. US FDA: Guidance for Industry and FDA Staff: Deciding When to Submit a 510(k) for a Software Change to an Existing Device, 2017.
6. US FDA: Guidance for Industry and FDA Staff: Guidance for the Content of Premarket Submission for Software Contained in Medical Devices, 2005.
7. ISO 14971:2007, Medical devices - Application of risk management to medical devices
8. 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.
9. ANSI/AAMI TIR57:2016, Principles for medical device security-Risk management
10. UL 2900-1:2017, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
11. 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

12. HIMSS/NEMA Standard HN 1-2013, Manufacturer Disclosure Statement for Medical Device Security form (MDS^2)