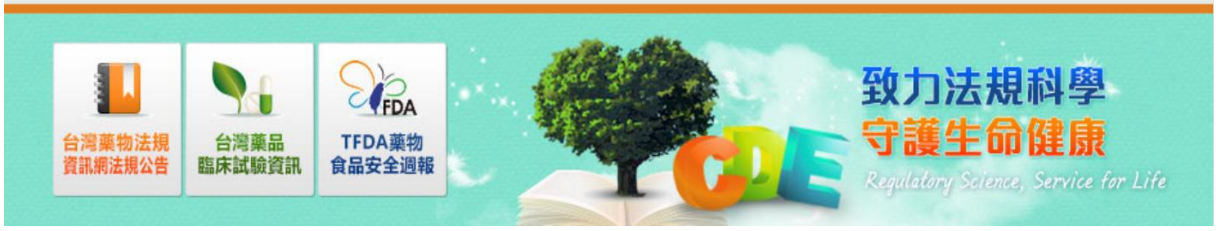
財團法人醫藥品查驗中心 Center for Drug Evaluation, Taiwan 當代醫藥法規月刊 2019-06-10 104
回 CDE 官網首頁
訂閱/取消電子報



美國醫療器材網路安全管理法規之沿革

盧巍[1]

前言

近二十年來，網際網路已經全面改變人類的生活，也促使了醫療產業逐漸朝向數位、遠距及行動三大領域蓬勃發展。網際網路與醫療器材的結合不僅便利了醫療院所對於資訊的儲存、傳遞與分析，也讓使用者能夠以無線的方式使用醫療器材及獲取相關資訊，提升使用的便利性。

然於 2012 年，美國知名駭客 Barnaby Jack 公開展示入侵遙控胰島素幫浦並控制施打劑量的過程，甚至表示可入侵心臟起搏器並釋放致命電壓，種種舉動證明有心人士若對醫療器材進行非法訊號存取，將嚴重危及病人的生命，也使得美國政府部門與國際大廠開始正視醫療器材可能存在的網路安全脆弱性(Cybersecurity vulnerabilities)。為此，美國食品藥物管理局(FDA)遂於 2013 年開始研擬《醫療器材上市前網路安全管理指引》(Content of premarket submissions for management of cybersecurity in medical devices)的初版草案，並於 2014 年頒布實施成為正式指引，提供製造廠有效管理網路安全的相關建議，進而維護醫療器材的安全性及有效性，也降低使用者可能承擔的風險。

於 2018 年，有鑑於日益增加的網路安全威脅需要更嚴謹的規範進行應對，FDA 發佈上述《醫療器材上市前網路安全管理指引》之修正草案。此修正草案除建立更清楚的網路安全管理架構，也更嚴謹地規範醫療器材網路安全的上市前要求，期望引領業界在設計與製造過程中有更加完善的網路安全法規可依循。

承上所述，本文將以 2018 年指引草案(以下簡稱 2018 年草案)為主軸，與 2014 年網路安全指引(以下簡稱 2014 年指引)內容作比較，釐清美國醫療器材網路安全管理的法規最新法規要求趨勢。

[1] 財團法人醫藥品查驗中心醫療器材組

美國網路安全管理指引比較分析

相較於 2014 年指引，FDA 於 2018 年草案提出數個網路安全新觀念以健全整體網路安全管理架構，包含：醫療器材網路安全風險等級、網路安全物料清單(Cybersecurity bill-of-materials, CBOM)、值得信賴醫療器材(Trustworthy device)及標籤建議(Labeling recommendations)等，同時將新觀念帶入產品設計與上市前申請文件的要求。FDA 將 2018 年草案分成：

I. 一般原則與醫療器材之網路安全風險評估

II. 設計「值得信賴醫療器材」：NIST 網路安全框架核心的應用

III. 具網路安全風險之醫療器材標籤建議

IV. 網路安全文檔(上市前申請文件)

以下，將就各章節依序說明 2018 年草案與 2014 年指引內容的差異。

I. 一般原則與醫療器材之網路安全風險評估

自 2014 年指引頒布實施至今，FDA 始終認為醫療器材的網路安全監督是製造廠、經銷商、醫療院所人員及使用者的共同責任。其中，身為產業鏈上游的製造廠，其責任在於設計開發一系列具備網路安全架構的醫療器材，同時依循品質系統法規 (Quality system regulation, QSR)之設計控制規範(21 CFR 820.30(g)-Design controls)進行測試，確保醫療器材具備辨識與處理「威脅(Threats)和脆弱性(Vulnerabilities)」的能力，以符合使用者需要及產品預期用途。

然於 2018 年修訂草案時，FDA 理解到單純的規範「威脅和脆弱性」並不足以確保醫療器材的安全性及有效性，故於修訂草案中納入醫療器材網路安全風險等級、網路安全物料清單(CBOM)等概念，藉此引導製造廠採用基於風險管理的方法，設計並開發具有適當網路安全保護的醫療器材，並對醫療器材全生命週期之網路安全風險和其緩和措施(Mitigation)進行評估，以持續確保醫療器材的安全性和有效性。

一、醫療器材網路安全風險等級

醫療器材若可與其他器材相連接(以無線或有線方式)、可插入攜帶式儲存裝置(如：USB 或 CD) 或可與網際網路連接，則比不具對外連接能力的醫療器材更容易受到網路安全的威脅。有鑑於此， 2018 年草案新增醫療器材「網路安全風險等級」之定義，其中包括：

(一) 高程度風險：

具備與「外部」連結能力的醫療器材，包含以有線或無線方式連結至其它醫療器材、非屬醫療器材之裝置或網際網路，且若發生網路安全事件，可能直接造成病人傷亡者。

具體示例包含：植入式心臟除顫器、心臟起搏器、腦刺激器、胰島素幫浦等，而與前述裝置連動的系統器材亦屬此類。

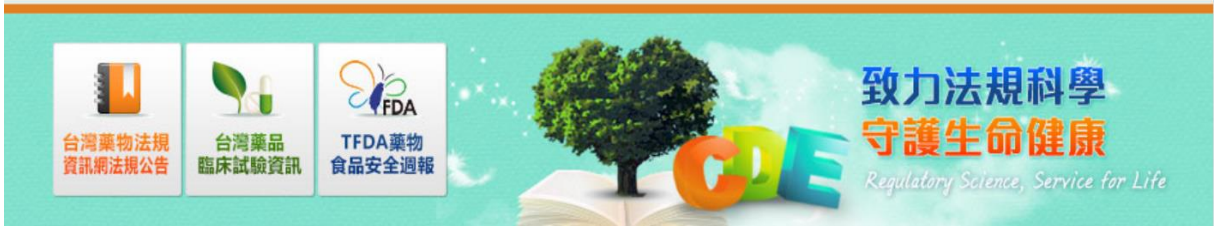
(二) 標準程度風險：

不符合上述「高程度風險」分類的醫療器材，則屬標準程度風險。

藉由以上定義產生之「醫療器材網路安全風險等級」，有助於製造廠在設計製造時進行合理的網路安全管控，且亦能指引製造廠於上市前申請時提交適當且完善的網路安全管理文件。此外，此風險分級方式不等同於美國聯邦法規法典第 21 冊(21 CFR)的醫療器材分級分類描述。舉例來說，不具連網性的冠狀動脈支架(高風險性醫療器材)，其「醫療器材網路安全風險等級」將低於可遠端遙控的胰島素幫浦(中風險性醫療器材)。

二、網路安全物料清單(CBOM)

美國 FDA 於 2018 年草案新導入 CBOM 的概念。所謂 CBOM 為一清單，詳列包含(但不限於)商用軟體、開放原始碼軟體及市售套裝軟體，和硬體組件內容。此清單功能在於引導製造廠識別其資產、威脅和責任。同時製造廠可透過 CBOM 的建立，達到確實遵守品質系統法規(QSR)的採購控制規範(21 CFR 820.50)、審慎評估材料供應鏈，建立並保存採購數據及資料，以管控任何影響產品安全的變更，達到確保產品網路安全的目的。CBOM 的導入，可協助製造廠進行網路安全風險評估與管理，同時 CBOM 也是上市前申請所需檢附的風險管理文檔之一，有助於 FDA 於產品於上市前審查時，了解其是否滿足於所適用的法規標準。



II. 設計「值得信賴醫療器材」: NIST 網路安全框架核心的應用

2014 年指引中，FDA 參考國家標準暨技術研究院(National Institute of Standards and Technology, NIST) 原針對國家關鍵基礎設施所發布之網路安全框架(Cybersecurity Framework, CSF)，並引用其中的五項核心(Core)作為醫療器材的網路安全設計概念，此五項核心分別為：識別(Identify)、保護(Protect)、偵測(Detect)、應變(Respond)及復原(Recover)。

2018 年草案中，FDA 導入「值得信賴醫療器材」的新觀念，並於產品設計的規範增編五項 CSF 核心，協助製造廠對於產品及其網路安全控制項目進行設計。同時也引導製造廠於後續上市前申請時，參照前述之「醫療器材網路安全風險等級」，提交具備「值得信賴醫療器材」特色的網路安全框架核心設計文件。

一、值得信賴醫療器材(Trustworthy device)

FDA 於 2018 年草案說明所謂「值得信賴醫療器材」應俱備以下特色：

- 面對網路安全相關入侵及濫用具有相當的防禦性。
- 能提供合理程度的可靠性和可用性，且可合理地被正確操作。
- 可合理且合適地執行其預期功能。
- 能遵守被廣泛接受的安全程序。

此外，FDA 認為在相關文檔中說明醫療器材的可信賴度，將有助於 FDA 更有效、快速地評估該醫療器材在網路安全方面的安全及有效性。

二、網路安全框架核心(Cybersecurity framework core, CSF core)

針對五項網路安全框架核心：識別(Identify)、保護(Protect)、偵測(Detect)、應變(Respond)及復原(Recover)，FDA 於 2014 年指引僅概略說明對應之要求，包含：

- 針對產品識別(Identify)、保護(Protect)功能，僅提及應「防止未經授權的使用者進行存取」與「確立內容的可信度」之相關要求。
- 針對產品偵測(Detect)、應變(Respond)及復原(Recover)功能，僅以下列四點規範：

1. 允許醫療器材在正常使用時，同步進行安全危害的偵測(Detected)、辨識(Recognized)、記錄(Logged)、時間控制(Timed)、處理(Acted)安全措施的功能。
2. 在檢測到網路安全事件時，提供使用者適當解決方法的相關資訊。
3. 產品應具備即便遭遇網路安全危害，仍能保護其關鍵功能的特色。
4. 提供經身份驗證的高權限使用者保存和恢復醫療器材配置的方法。

相較於 2014 年指引，FDA 於 2018 年草案新增的考量如下：

- 針對產品識別(Identify)、保護(Protect)功能，除原有規範內容外，應另具備保護資產及其功能性的能力，並以維持來往資訊的鑑別性(Authenticity)、可取得性(Availability)、完整性(Integrity)及機密性(Confidentiality)為主要目標，降低使用者可能承受的風險。
- 針對產品偵測(Detect)、應變(Respond)及復原(Recover)功能，應增加其規範內容，更嚴謹地規範產品應設計成具有預測及應對動態網路安全風險的能力，包括：針對網路安全的例行更新(Updatability)與修補(Patches)、緊急應變措施。

表一為兩指引於「網路安全框架核心」規範內容大綱比較。

表一、「網路安全框架核心」規範內容大綱比較

2018 年草案	2014 年指引
A. 識別(Identify)、保護(Protect)醫療器材資產及功能性	識別(Identify)、保護(Protect)
1. 防止未經授權的使用	△
(a).防止未經授權的使用者及醫療器材進	防止未經授權的使用者進行存取

行存取	
(b).驗證和檢查安全關鍵命令的授權	△
2. 確立內容的可信度-確保密碼，數據和執行程序的完整性	確立內容的可信度
(a).程式完整性	(編按：針對程式完整性， 2014 年指引要求製造廠考慮採用「程式碼簽章憑證(Code signature verification)」的認證方式來限制軟體及韌體的更新，並使用系統程序方式，使被授權的用戶能下載可識別版本的軟體及韌體。然而，此項要求已於 2018 年草案中刪除，FDA 改建議其他方式以達到資料之完整性。)
(b).資料完整性	(編按： 針對資料完整性， 2014 年指引僅建議應針對資料傳輸的過程進行加密驗證，以確保器材安全地數據傳輸)
(c).執行完整性	△
3. 維持資料的機密性	△
B. 偵測(Detect)、應變(Respond)及復原(Recover)-預期設計	偵測(Detect)、應變(Respond)及復原(Recover)
(a).使產品能及時檢測網路安全事件	● (編按： 於 2014 年指引未有對應之完整章節說明相關內容，僅要求允許器材在正常使用時，同步進行偵測

	(Detected)、辨識(Recognized)、記錄(Logged)、時間控制(Timed)、處理(Acted)安全措施的功能。)
(b).使產品能應對並遏制潛在網路安全事件的影響	● (編按： 於 2014 年指引未有對應之完整章節說明相關內容，僅要求器材在檢測到網路安全事件時，能為終端使用者提供適當解決方法的資訊。)
(c).使產品能恢復因網路安全事件而受損的功能或服務	● (編按： 於 2014 年指引未有完整章節說明相關內容，僅要求設計上，即使器材的網路安全受到損害，器材仍需具備保護其關鍵功能的能力。並需提供經過身份驗證的高授權用戶保存和恢復器材配置的方法。)
△(無相關內容規範)	

以下就表一刊載之大綱內容順序，逐項說明各項核心所要求之產品設計要求。

A. 識別(Identify)、保護(Protect)醫療器材資產及功能性

FDA 為防止醫療器材及系統的鑑別性(Authenticity)、可取得性(Availability)、完整性(Integrity)及機密性(Confidentiality)降低而對多數病人造成傷害，故提供了有關身份驗證，授權和加密的設計建議如下。

1. 防止未經授權的使用

(a).防止未經授權的使用者及醫療器材進行存取

(1) 透過驗證使用者身份，限制醫療器材的存取權限（如：使用者 ID 和密碼，智慧卡，生物辨識技術）。

(2) 使用自動「時間控制」方法，於使用環境下自動終止系統內的工作階段。

(3) 採用「分層授權模型」，透過使用者身分（如：護理人員、病人、照護者、系統管理員）或醫療器材功能來區分存取權限。

(4) 使用妥善的驗證方式（如：多因素認證(Multi-factor authentication)，給予特殊身分者如：系統管理員，技術人員及維護人員存取權限）。

(5) 加強密碼保護，避免使用常態性或容易被破解的密碼(如：於多項醫療器材使用相同密碼、自動記憶密碼、無法或難以變更的密碼或強度脆弱而易猜的密碼)，並避免於公共場合重複使用任何用於特殊醫療器材的密碼。

(6) 考慮在醫療器材及其連接埠外裝置實體的鎖鑰，以降低被篡改的風險。

(b).認證和檢查安全關鍵命令的授權

(1) 使用驗證機制以防止未經授權的醫療器材之存取、未經授權之軟體執行。

(2) 進行軟體及韌體(包含可能影響系統操作的軟體及韌體、應用程式及防毒軟體)更新之前，需經使用者的身份驗證，此項目為 2014 年指引既有規範，而 2018 年草案續保留編列於此。

(3) 於醫療器材上使用強化的加密認證法，進行人員身分、訊息、命令以及所有其他通訊路徑(如適用)的認證。

(4) 醫療器材所有對外的連線皆需進行驗證，舉例來說，如果醫療器材連接至外部伺服器，即使這個連接是經由一個或數個已經存在的可信任通道，醫療器材本身及伺服器仍須進行交互認證。

(5) 透過軟體及韌體內容的標記對其進行驗證，如：數位簽章(Signatures)、訊息鑑別碼（Message Authentication Codes, MACs））、版次號碼或詮釋資料(Metadata)等資訊。且預計安裝的軟體版次應有數位簽章或訊息鑑別碼，而醫療器材應有數位化資訊(如：產品型號、序號)供授權使用者辨識。

(6) 根據授權憑證或同等級的驗證資訊執行授權檢查，如：醫療器材程式的設計者，其權限應經過加密認證保護，或者該權限在受到軟體攻擊時無法被其它器材

(如：家用螢幕)所複製。

(7) 醫療器材應設計為「默認拒絕(Deny by default)」模式，意即醫療器材應預設成自動拒絕連接未經允許的線路或其它裝置，如：傳輸控制協定(TCP)、USB、藍芽及序列通訊。

(8) 僅執行器材基礎功能的權限，應以最低權限原則來規範。

2. 確立內容的可信度-確保密碼，數據和執行程序的完整性

於 2014 年指引中，FDA 刊載以下三點作為「確立內容可信度」的規範：

(1) 製造廠可考慮採用「程式碼簽章憑證(Code signature verification)」的認證方式來限制軟體或韌體的更新。

(2) 採用系統程序方式，使被授權的使用者能從官方網頁或連結下載可識別版本的軟體及韌體。

(3) 可考慮採用加密方法，確保數據於醫療器材間可以安全地傳輸。

而於 2018 年草案中，FDA 將上述第(1)、(2)點移除，僅保留上述第(3)點。此外，FDA 針對「確立內容的可信度」新增以下規範。

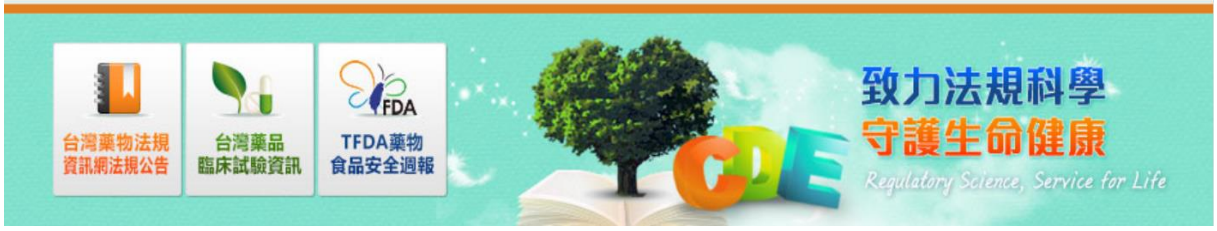
(a).程式完整性

(1) 僅允許安裝經過加密認證的軟/韌體的更新檔。使用經加密簽章的更新檔來確保軟體版本維持在最新狀態，有助於防止醫療器材在未經授權情況下降低保護層級(降級或回滾攻擊, Downgrade or Rollback attacks)。

(2) 在可行的情況下，確保軟體在執行前其完整性已經驗證，如：具數位簽章的白名單(Whitelisting，編按： 為特定的電子郵件來源名單，特別容許該來源的電子郵件進入收件匣)。

(b).資料完整性

(1) 驗證所有接收資料的完整度，確保資料於暫存或傳輸的過程中未被竄改，並



仍可完善執行預期的程序或符合預期的規格。

(2) 確保醫療器材可安全地傳輸數據，如果合適的話，使用加密方法及對於資料傳輸的目的地進行認證。此項 2014 年指引已作要求，而 2018 年草案進一步將「對資料傳輸的目的地進行驗證」內容，將其列入資料完整性的考量項目。

(3) 對於醫療器材安全性及有效性重要的資料，應保護其完整性。

(4) 以 NIST 所建議之網路安全標準或同等強度標準以加密保護醫療器材間的連線。

(5) 針對醫療器材使用獨立加密安全通訊密鑰，防止單一密鑰被破解後於多個醫療器材登入。

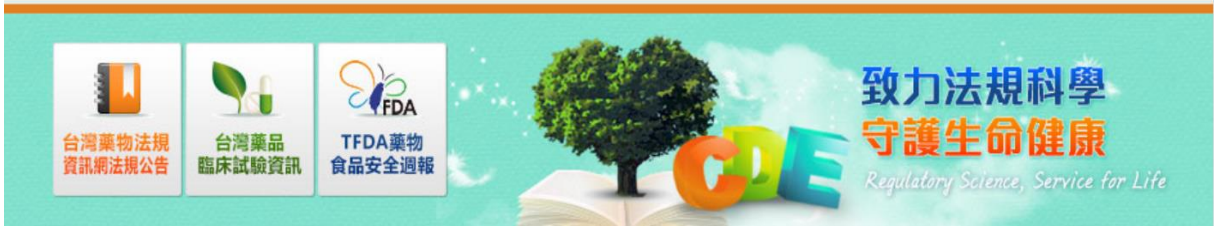
(c).執行完整性

可行情況下，當醫療器材執行程式碼時，應採用業界公認最佳的方式來維護或驗證程式碼的完整性。

3. 維持資料的機密性

在 2018 年草案，FDA 規範製造廠應採用「憑證」或「加密」的方式維持資料的機密性，以避免對病人可能導致傷害的任何資料被揭露。兩種方式皆有其重要性，若無法維持「憑證」的機密性，則許多病人都將受到傷害。而若資料於暫存或傳輸的過程缺乏「加密」機制對敏感資訊進行保護，則可能導致資訊被濫用而造成病人傷害(Patient harm)。

此外，2018 年草案規範範疇並未涵蓋受保護健康資訊(Protected health information, PHI)，這是因為 FDA 認為未能有效維護 PHI 的機密性並不被視為造成「病人傷害」。然而，FDA 提醒仍須依照適用的聯邦法和州法(包括健康資訊可移植性和責任法案, HIPAA)，在產品全生命週期中，製造廠和(或)其他產品使用單位仍有義務根據不同的情形，對 PHI 的有效性、完整性與機密性進行維護。



B. 偵測(Detect)、應變(Respond)及復原(Recover)-預期設計

1. 使產品能及時檢測網路安全事件

(1) 允許醫療器材在正常使用時，同步進行安全危害的偵測(Detected)、辨識(Recognized)、記錄(Logged)、時間控制(Timed)、處理(Acted)安全措施的功能。此項目為 2014 年指引既有規範，而 2018 年草案續保留編列於此。

(2) 產品須設計為允許例行性的安全和防毒掃描，避免影響醫療器材的安全性和有效性。

(3) 產品的設計需確保能夠保留資安鑑識證據。設計的機制應具備根據安全事件創建、存儲記錄檔。記錄檔內容應包括： 記錄檔的位址、如何儲存、回收或封存，以及自動分析軟體(如：入侵檢測系統(Intrusion Detection System, IDS)) 如何讀取記錄文件進行分析識別。偵測之安全事件則應包括配置改變(Configuration changes)、網路異常、登錄嘗試和異常流量(如：對未知單位提出存取要求)等。

(4) 產品設計應有明確的安全配置以限制脆弱性的潛在影響。安全配置可以包括端點保護，如：防毒軟體、防火牆及其規則、白名單、定義安全事件參數、記錄檔參數或實體的安全檢測。

(5) 產品應設計可啟用「軟體配置管理」，並允許授權使用者以電子化獲取的方式 (意即機器可讀, Machine readable)追蹤和控制軟體的變化。

(6) 產品其生命週期(包含產品設計)，應利於對醫療器材型號和產品線之中的脆弱性進行多重分析。

(7) 產品設計上應提供機器可讀且具電子化格式的 CBOM，以便醫療器材內部執行時自動分析利用。

2. 產品設計能應對並遏制潛在網路安全事件的影響

(1) 在檢測到網路安全事件時，醫療器材應提供使用者適當解決方法的相關資訊。此項目為 2014 年指引既有規範，而 2018 年草案續保留編列於此。

(2) 醫療器材應設計成可進行軟體修補及更新，以解決未來可能的網路安全脆弱性。

(3) 醫療器材應設計為便於進行(快速)驗證、確效和測試軟體修補及更新。

(4) 設計架構應有助於軟體修補及更新檔的快速安裝。

3. 使產品能恢復因網路安全事件而受損的功能或服務

(1) 產品應具備即便遭遇網路安全危害，仍能保護關鍵功能的特色。此項目為2014 年指引既有規範，而 2018 年草案續保留編列於此。

(2) 提供經身分驗證的高授權使用者保存和恢復器材配置的方法。此項目為2014 年指引既有規範，而 2018 年草案續保留編列於此。

(3) 醫療器材系統組件應具備適應組件間長時間中斷連線情形的能力。

(4) 醫療器材需能適應潛在的網路安全事件，如：中斷網路、阻斷服務攻擊（Denial of service, DoS）、頻寬過載、網路連線服務品質(Quality of service, QoS)的破壞和過度訊號抖動情形（Excessive jitter, 即接收數據過程中的延遲變異情形）。

III. 具網路安全風險之醫療器材標籤建議

FDA 規範醫療器材之「標籤」乃根據聯邦食品、藥品、化妝品法案(FD&C Act)而執行，其中於 502(f)、502(a)及 201(n)，主要敘述標籤的適當性與錯誤標籤定義，而於 21 CFR 801.5、801.109(c)，則分別規範對於一般使用者及專業技術人員應標明之訊息，如：醫療器材所有操作條件、目的或用途(包含：危險、警告、預防措施、禁忌症等)。

於 2018 年草案中，FDA 考量具有網路安全風險的醫療器材，其「標籤」應提供使用者與網路安全風險相關的注意事項，遂新增於 2014 年指引未包含之章節「標籤建議」，要求製造廠應考量如何制訂合適的「標籤」以含括產品的資安設計、使用方法、產品架構等資訊，充分向使用者傳達以下資訊：

1. 針對預期使用環境所推薦的網路安全控制措施（如：防毒軟體，防火牆），應提供使用者相關之醫療器材簡介和產品規格說明。

2. 描述產品特色，說明醫療器材的網路安全即便受到侵害，也能保護其關鍵功能。

3. 說明產品備份和還原功能，以及如何恢復產品原始配置的過程。

4. 關於網路基礎架構的配套措施，應提供使用者具體指引以便醫療器材可以按預期運作。

5. 描述產品目前所使用或可新增的安全配置，包括：防毒軟體，防火牆/防火牆規則、白名單、安全事件參數、登錄記錄參數或物理安全檢測等保護機制。

6. 提供接收/發送數據的網路連接埠(Network ports)或其它介面(Interfaces)的清冊，描述連接埠用於資料的傳入或傳出，並將未使用的連接埠予以禁用。

7. 提供被授權使用者系統更新流程與方法，說明如何從製造廠下載可識別版本的軟體及韌體。

8. 描述醫療器材在檢測到異常情況(網路安全事件)時的通知設計。網路安全事件類型包括：配置改變、網路異常、登錄嘗試、異常網路流量(如：向未知使用者發出要求)。

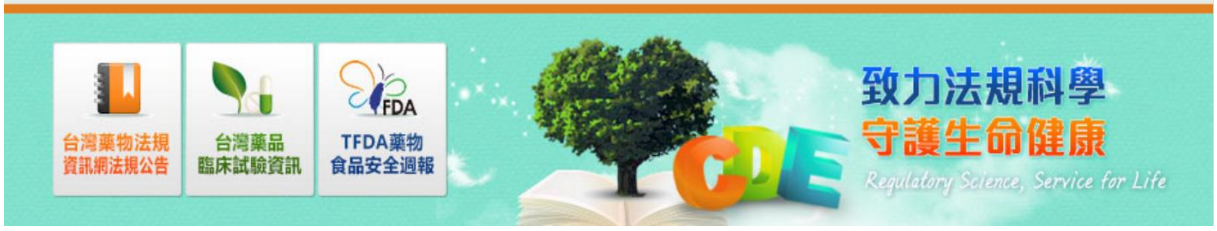
9. 描述鑑識證據的記錄擷取方式，包括(但不限於)基於網路安全事件所保留的任何記錄檔。記錄檔內容應包括： 記錄檔的位址、如何儲存、回收或封存，以及自動分析軟體 (如：入侵檢測系統(Intrusion Detection System, IDS)) 如何讀取記錄文件進行分析識別。

10. 描述經身份驗證的特權使用者保存和恢復醫療器材配置的方法。

11. 提供使用者詳細的醫療器材系統圖。

12. 提供 CBOM 清單，其應包含(但不限於)商用軟體、開放原始碼軟體及市售套裝軟體，和硬體組件，使醫療器材使用者如：病人、供應商和醫療院所能夠有效地管理其資產，了解已識別之脆弱性對醫療器材以及連接系統的潛在影響，並研擬維護醫療器材基本性能的對策。

13. 適時提供使用者安全連網配置和服務的技術說明，引導使用者於發生網路安全



脆弱性或事件時及時作出反應。

14. 提示使用者，於製造廠中止提供安全軟體修補或更新的服務後，若仍繼續使用該醫療器材，則使用者的網路安全風險可能會隨著時間的而增加，故需多加留意醫療器材於製造廠中止服務(End of support)後的醫療器材網路安全。

IV. 網路安全文檔(上市前申請文件)

於 2014 年指引中，針對上市前申請應提交之網路安全文件，FDA 僅提出五點建議：

1. 提供網路安全分析報告，詳述與產品相關的網路安全風險及危害，以及所設計的解決方法及考量因素
2. 提供可追溯矩陣圖，將產品設計之網路安全控制項目與所對應之預期風險作連結對應。
3. 提供摘要，說明於產品全生命周期提供驗證的軟體和修補的更新計劃，以及如何持續確保醫療器材的安全性和有效性。(若為加強網絡安全而進行的醫療器材軟體更新，則不需經過 FDA 審查或批准。)
4. 提供風險管控摘要，說明如何確保醫療器材從製造廠到使用端(醫護、病人)之間，皆能保持其完整性，如：保持無惡意軟體。
5. 針對預期使用環境所推薦的網絡安全控制措施（如：防毒軟體、防火牆），應提供使用者相關之器材簡介和產品規格說明。

而於 2018 年草案中，FDA 除保留上述 2014 年指引的內容外，進一步將上市前申請文件細分為「產品設計文檔」與「風險管理文檔」兩大類，並增列對應要求。

A. 產品設計文檔

在「產品設計文檔」，此部份保留上述 2014 年指引之第 3 點內容，並要求產品設計文檔應包含三部份：對應網路安全風險等級的產品設計文件、系統圖(System diagrams)及設計功能摘要，以利說明產品基於風險的產品設計和所設置網路安全防禦水準的適當性。

1. 對應網路安全風險等級的產品設計文件

FDA 建議製造廠根據醫療器材之「醫療器材網路安全風險等級」提供符合值得信賴醫療器材特色及 CSF 核心架構的產品設計文檔。

(一) 高程度風險

若為高程度風險之醫療器材，需根據五項核心：識別(Identify)、保護(Protect)、偵測(Detect)、應變(Respond)及復原(Recover)，提交符合其核心架構的所有產品設計文件，如前述章節「II 產品功能與設計」。

(二) 標準程度風險

標準程度風險的醫療器材，將可改以基於風險管理的說明文件，解釋不需進行網路安全設計監控的緣由，而無須檢附五項核心架構所要求的所有文件。

2. 系統圖(System diagrams)

FDA 建議，製造廠以系統圖呈現「II.產品功能與設計」內容並整合為系統層級和樹狀圖，可協助衛生主管機關對整個產品系統進行分析。FDA 認為，系統圖應含以下內容：

(1) 網路、架構、流程和狀態圖。
(2) 介面、組件、資產、通訊路徑、通訊協定和網路連接埠。
(3) 包括網站、伺服器、互動式系統及雲端商店等通訊資產或系統組件的驗證機制和管控方式。
(4) 使用者於使用資產及通訊通道時的角色定位與責任。
(5) 加密方法之描述應包含採用之方法、密鑰(Cryptographic key)使用的類型與層級以及在整個系統中的使用方式(如：一次性使用、密鑰長度、採認標準、金鑰對稱性或其他方式等)。且應詳述與軟/韌體更新相關的加密保護細節。

3. 設計功能摘要

相較於 2014 年指引內容，2018 年草案修正強調設計功能摘要應針對可使軟體在其全生命週期進行必需之更新與修補的「產品設計特色」進行說明；此外，本次亦刪除 2014 年指引內容：若僅為加強網絡安全而進行的醫療器材軟體變更，則通常不須經過

FDA 的審查或批准。(內容比較呈現於下表二)

表二、設計功能摘要比較

2018 年草案	2014 年指引
提供描述產品設計特色之摘要，說明如何於產品全生命周期中，提供所需之驗證軟體和修補，持續確保醫療器材的安全性和有效性。	提供摘要，說明於產品全生命周期中提供驗證軟體和修補的規劃，持續確保醫療器材的安全性和有效性。 若僅為加強網絡安全的醫療器材軟體變更，則通常不須要經過 FDA 的審查或批准。

B. 風險管理文檔

在 2018 年草案「風險管理文檔」的要求中， FDA 除保留上述 2014 年指引內容(第 1, 2, 4, 5 點)，另建議製造廠將產品設計與威脅模型、臨床危害、降低風險的措施和產品試驗結合，建立一個安全的設計架構來進行風險管理。

1. 系統層級威脅模型(System level threat model)

在 2018 年草案新增內容中，FDA 建議製造廠建立系統層級威脅模型，將各系統層級的風險，包括(但不限於)供應鏈相關的風險（如：確保產品維持無惡意軟件）、產品設計、生產和連線配置（如：連線或連網環境）均納入風險考量，並保留其中對於產品完整性的要求(如：確保產品維持無惡意軟體)。而原 2014 年指引所列「針對預期使用環境所推薦的網路安全控制措施（如：防毒軟體，防火牆），應提供使用者相關之器材簡介和產品規格說明」之內容(如表三)，則於 2018 年草案編列至「III. 網路安全風險醫療器材的標籤建議」進行規範。

表三、系統層級威脅模型-產品完整性要求的內容比較

2018 年草案	2014 年指引
提供製造廠建立系統層級威脅模型，將各系統層級的風險，包括(但不限於)供應鏈相關的風險（如：確保產品維持無惡意軟件）、產品設計、生產和連線配置（如：連線或連網環境）均納入風險考量。	製造廠應提供風險管控摘要，說明如何確保醫療器材從製造廠到使用端(醫護、病人)之間，皆能保持其完整性，如：確保產品維持無惡意軟體。

2. 網路安全分析報告

FDA 於 2014 年指引並未說明網路安全風險與控制的具體做法，僅要求製造廠提供網路安全分析報告，詳述產品可能受到之意圖(Intentional)或非意圖(Unintentional)的網路安全風險及危害，以及所設計的解決方法及考量因素。網路安全分析報告包含：

- 網路安全風險清單，具體詳述設計中考慮的所有網路安全風險。
- 網路安全控制清單，具體詳述為醫療器材建立的所有網路安全控制的理由。

於 2018 年草案，FDA 則提供了具體的網路安全風險與控制報告的方法，引導製造廠於上市前申請更加有所依循。

- 網路安全風險清單，除應具體詳述設計中考慮的所有網路安全風險外，FDA 建議製造廠提供風險描述，並採用「可開發性分析」取代「機率」來描述風險發生的可能性。然若製造廠提供了發生風險的機率值，FDA 則建議製造廠應提供計算方式來說明解釋。
- 網路安全控制清單，除應具體詳述為醫療器材建立的所有網路安全控制的理由外，報告內容應含括與醫療器材之相關網路安全風險，以及所有風險緩解和產品設計的考慮因素，包括：

  a. 與存取控制、加密/解密、防火牆、入侵檢測/預防及防毒軟體等相關的可驗證功能/子系統列表。

b. 對其他功能性、數據和連接埠需求造成影響的可驗證安全措施列表。

3. 網路安全風險測試報告

為確保妥善的進行網路安全風險控制，FDA 於 2018 年草案新增要求製造廠提供相關風險控制測試的描述，如：執行特定安全政策的效益、所需傳輸條件下的產品性能或穩定性和可靠性等。建議具體之風險測試報告內容應包括：

(1) 測試醫療器材性能
(2) 系統中第三方之防毒軟體其安全及有效性的證據
(3) 靜態和動態密碼分析，包含常態性、預設的、過於簡易的、易破解的密碼的測試
(4) 脆弱性掃描
(5) 穩健性測試
(6) 邊界分析
(7) 滲透測試
(8) 第三方測試報告

4. 可追溯矩陣圖

2014 年指引建議製造廠提交可追溯矩陣圖，將實際的「網路安全控制項目」連結對應至「考量之風險」。而 2018 年草案則具體說明製造廠「考量之風險」應基於「安全風險(Security risk)與危害分析(Hazard analysis)」之結果提出。

5. CBOM

針對 2018 年草案新提出的 CBOM 概念，FDA 建議此 CBOM 應與國家脆弱性數據庫 (National vulnerability database, NVD) 或類似的「已知脆弱性」(Known vulnerability)資料庫進行交叉比對，並提供「已知脆弱性」的排除標準及不排除的理由。

結語

由 2018 年草案可見美國 FDA 對於醫療器材的「網路安全管理」隨著科技的快速發展而漸趨嚴謹，然本次修訂並非只嚴格要求製造廠遵守相關規範，FDA 在提出全新觀念的同時，也針對 2014 年指引內容有更加詳盡明確的說明，因此製造廠也將更了解具潛

在網路安全風險之醫療器材，並於其產品從設計開發、生產製造到上市申請階段，有更明確的方向可依循。

參考文獻

1. Content of premarket submissions for management of cybersecurity in medical devices： Guidance for industry and food and drug administration staff (2014)
2. Content of premarket submissions for management of cybersecurity in medical devices : Draft guidance for industry and food and drug administration staff (2018)