正本

檔　　號：
保存年限：

衛生福利部食品藥物管理署　函

地址：115209臺北市南港區昆陽街161-2號
聯絡人：簡俊仁
聯絡電話：02-27877551
傳真：02-26532005
電子郵件：i64901037@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 111. 06. 13 文
檔號: 111310

裝

發文日期：中華民國111年6月9日
發文字號：FDA器字第1111601837號
速別：普通件
密等及解密條件或保密期限：
附件：行動醫療科技醫療器材上市前審查網路安全問答集、醫療器材軟體上市後變更申請常見問答集

主旨：本署研訂「行動醫療科技醫療器材上市前審查網路安全問答集」、「醫療器材軟體上市後變更申請常見問答集」及「醫療器材網路安全評估分析參考範本」新增品項範本，請貴會協助轉知所屬會員，詳如說明段，請查照。

訂

說明：

一、為提供各界行動醫療科技醫療器材上市前查驗登記申請及醫療器材軟體上市後變更申請之參考及提升醫療器材網路安全，增進我國醫療器材商申請查驗登記時準備網路安全文件之時效，本署參酌國際間指引標準及我國「醫療器材軟體上市後變更申請之管理指引」等，研訂旨揭問答集及範本供各界於規劃行動醫療科技醫材上市前、醫療器材軟體上市後變更及網路安全評估實務撰寫之參考。

線

二、旨揭範本內容請至本署全球資訊網站(http://www.fda.gov.tw/)(首頁> 業務專區> 醫療器材> 法規專區>其他)及智慧醫療器材資訊平台(http://imdis.fda.gov.tw)下載。

正本：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、屏東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、中華民國儀器商業同業公會全國聯合會、嘉義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、桃園市儀器商業同業公會、新竹市儀器商業同業公會、臺南市儀器商業同業公會、中華生物醫學工程協進會、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、財團法人台灣商品檢測驗證中心、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、台灣醫療器材門市發展協會、中華民國生物產業發展協會、中華民國全國商業總會、中華民國全國工業總會、台灣先進醫療科技發展協會、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、台灣科學工業園區科學工業同業公會、科技部中部科學園區管理局、科技部南部科學園區管理局、南港軟體工業園區二期管理委員會、台灣區電機電子工業同業公會、台灣臨床檢驗標準協會、台灣藥物臨床研究協會、財團法人資訊工業策進會、中華民國生物醫學工程學會、財團法人生技醫療科技政策研究中心、社團法人台灣醫學資訊學會、台灣醫院協會、社團法人台灣生醫電子工程協會、財團法人工業技術研究院生醫與醫材研究所、臺灣美國商會、歐洲在台商務協會、台北市日本工商會、台灣醫療暨生技器材工業同業公會、中華民國資訊軟體協會、台北市電腦商業同業公會、台灣顯示器產業聯合總會、台灣健康資訊產業整合協會、台灣健康資訊交換標準第七層協定協會、台灣數位安全聯盟、財團法人中華民國國家資訊基本建設產業發展協進會、社團法人台灣電子設備協會、台灣生技醫療照護輔具協會、台灣醫療照護輔具協會、社團法人臺灣輔具產業發展協會

副本：

署長 吳秀梅

行動醫療科技醫療器材上市前審查網路安全問答集

111 年 3 月

一、前言

為協助業者了解我國行動醫療科技醫療器材上市前審查網路安全需求，搭配衛生福利部食品藥物管理署 110 年 12 月 6 日公布之「醫療器材網路安全評估分析參考範本」，特撰擬本問答集以協助業者解決在評估醫材網路安全及撰寫評估分析報告時常見問題，惟網路安全技術日新月異，業者仍應視產品及技術特性，妥善執行醫療器材網路安全評估。

二、常見問答集

Q1:

使用藍芽傳輸技術的醫療器材，若經過器材之間 BLUETOOTH LOW ENERGY (BLE)的綁定，使只有綁定過後的器材能夠接收、讀取，是否符合食藥署 110 年 5 月 3 日公告之「適用於製造業者之醫療器材網路安全指引」的範疇？

A1:

依據本署「適用於製造業者之醫療器材網路安全指引」基本原則，醫療器材應維護其機密性和完整性，各種技術的綁定屬一種授權行為，確保資料在授權的情況下才能被存取尚符合指引範疇；無論使用何種技術，皆可依據「適用於製造業者之醫療器材網路安全指引」並可參酌「醫療器材網路安全評估分析參考範本」評估其網路安全風險。

Q2:

經醫材量測後的資料，若被第三方 App 取用是否違反食藥署 110 年 5 月 3 日公告之「適用於製造業者之醫療器材網路安全指引」的範疇？

A2:

依據本署「適用於製造業者之醫療器材網路安全指引」基本原則，醫療器材應維護其機密性和完整性，第三方 App 在未經授權下，不

得取用資料，然若經過授權，並符合前開指引之機密性和完整性者，則無違反上開指引之疑慮。

Q3:

自定義的資料格式是否等同加密，例如此資料未使用特別的軟體無法讀取，或需使用業者本身的 PROFILE 格式，是否符合網路安全指引？

A3:

依據本署「適用於製造業者之醫療器材網路安全指引」基本原則，醫療器材應維護其機密性和完整性；加密所採用之演算法技術或是 profile 格式，應綜合考慮經網路安全評估後是否還有殘餘風險，若使用自定義資料格式就可達到加密效果且經評估後殘餘風險可接受，尚符網路安全指引中之醫療器材應維護其機密性和完整性部分；無論使用何種技術，皆可依據「適用於製造業者之醫療器材網路安全指引」並可參酌「醫療器材網路安全評估分析參考範本」評估其網路安全風險。

Q4:

在填寫醫療器材網路安全評估報告前，是否需先做風險評估的相關文件?例如：評估系統傳輸資料型態、若資料被破壞、竊取時，會對系統造成怎樣的風險等。

A4:

是，如同「醫療器材網路安全評估分析參考範本」中第 3.1.1 節“網路安全威脅建模方法”所示，第一項「識別資產」是指醫材項目中有哪些重要資產，例如使用者個人資料、演算法等，不管是內部或是外部傳輸的相關資料都屬於重要資產的範疇。第二項「資料流向圖(Data Flow Diagram, DFD) 」，資料流向圖會有所謂的信賴區間跟信賴邊界，來幫助理解產品資料流向與可控範圍，透過 DFD 圖能夠更理解資料的流向，並確保傳入目標的資料是可信賴或是沒經過竄改的，確認之後就可以找出相關的網路風險，並隨後於第 3.3 節”分析網路安全威

脅”，透過不同識別的資產分析每一項可能遭遇的威脅並且於威脅列表中羅列出來。

Q5:

漏洞掃描可否委外或是由業者自行執行?

A5:

漏洞掃描可委外第三方實驗室或業者自行建立之網路安全相關部門執行，測試人員需具相關經驗能力說明，委外或是由業者自行執行可依據業者自身狀況來決定。

Q6:

針對「醫療器材網路安全評估分析參考範本」第 2.2 節「網路安全要求檢核表」，請問項目中出現何種情形於表格上填「否」或是「不適用」?

A6:

此部分由業者依據產品開發時的內部設計來進行填寫。例如在機敏資料傳輸時，採用加密機制這項目中，若有採用就填寫「是」，沒有採用就填「否」。若是業者開發的醫療器材在應用情境中不須要考量，那就是填「不適用」。例如在輸入驗證中，輸入驗證外部取得的資料這項來說明，若系統沒有使用外部資料，那就是填「不適用」。

Q7:

如果在「醫療器材網路安全評估分析參考範本」第 2.2 節「網路安全要求檢核表」中某個項目為「否」，這樣此項目還需要列入網路安全要求(Security Requirement Specification, SRS)嗎?

A7:

如果業者所開發的醫療器材沒有此項目，且經評估為無或低風險，可以在網路安全風險評估說明無此風險或此風險極低可接受。

Q8:

按照「醫療器材網路安全評估分析參考範本」中的「網路安全要求檢核表」之機密性的第三條「使用公開、國際機構驗證且未遭破解的演算法」，請問雲端傳輸 SSL 符合這樣的演算法嗎?

A8:

採用何種演算法及資料加密的程度由業者自行決定，整體仍以醫療器材網路安全風險評估，依據剩餘風險是否可以接受，再來檢視調整演算法及資料加密的程度。

Q9:

根據「醫療器材網路安全評估分析參考範本」中的「網路安全要求檢核表」之機密性第五條「不使用自行創造的加密方式」，如果業者使用了自己創造的加密方式，是否需要自行驗證加密的強度?

A9:

依據本署「適用於製造業者之醫療器材網路安全指引」，醫療器材應維護其機密性和完整性；加密所採用之演算法技術或是 profile 格式，應綜合考慮經網路安全評估後是否還有殘餘風險，若使用自創加密方式應驗證其可以達到加密效果且加密強度足夠，並經評估後殘餘風險應為可接受。

Q10:

請問「醫療器材網路安全評估分析參考範本」中的「網路安全要求檢核表」的組態管理項目為何?

A10:

指軟體或是裝置的 config 檔案。也就是說要執行軟體或是裝置時後面所需要的軟硬體設置，像是 AI 參數、OS 設定檔等。

Q11:

請問網路安全要求(Security Requirement Specification, SRS)跟網路安全細部設計(Security Detail Design, SDD)內容一樣可以嗎？

A11:

網路安全細部設計(SDD)是業者實際在設計產品時如何達成網路安全要求(SRS)，可能多項 SDD 對應 1 項 SRS，並未強制一定要內容一樣。

Q12:

網路安全驗證確效測試(Security Validation & Verification, SVV)中的測試結果欄位可以放什麼來舉證？

A12:

可於測試結果欄位放入圖片、測試的結果、引述附件等，並應敘明測試結果為 Pass 或是 Fail。

Q13:

請問「醫療器材網路安全評估分析參考範本」中的威脅建模部分，其評估是否有既定的國際標準還是可以自行評估？

A13:

威脅建模的評估可參考國際組織標準或自行評估。亦可參考本署公布之「醫療器材網路安全評估分析參考範本」第 3.1.1 節網路安全威脅建模方法，包含「識別資產」、「資料流向圖(Data Flow Diagram, DFD) 」及「分析網路安全威脅」等流程執行。

Q14:

如果醫療器材產品使用者角色種類有多種，那資料流向圖(Data Flow Diagram, DFD)是否要增加呢？

A14:

是。但若不同角色做相同事情，可簡化流向圖並將其資訊備註。

Q15:

請問「醫療器材網路安全風險等級檢核表」中的弱點因素(V1)發現的難易度，其指的是使用者或是開發者？

A15:

使用者，發現難易度為視使用作業系統，例如若為主流設備或作業系統業者較能支援等，分數 1 分代表設備市占率高且業者能支援程式修補，或因作業系統客製化，攻擊意願較低者。

Q16:

如果某項威脅對於使用者的危害程度不高，應如何在「醫療器材網路安全風險等級檢核表」中填寫其影響程度(Impact Factor)呢？

A16:

若業者經評估此威脅對病人(使用者)危害程度很低，其影響程度可以填 1，但是有可能此威脅容易發生如資料竄改等情況，發生可能性為高，因此業者要揭露所有可能的網路安全風險影響到病人(使用者)的程度並確定其風險內容制定對應的管控措施，使風險降為可接受程度。

Q17:

請問「醫療器材網路安全評估分析參考範本」第 3.4 節「醫療器材網路安全風險等級檢核表」一定要按照上面的項目來做勾選嗎?

A17:

這部分需依據業者所開發的醫療器材所識別的資產來填寫，再根據這些資產可能遭遇的風險進行勾選跟填寫。

Q18:

如果漏洞掃描與滲透測試是委託某資安實驗室執行，是否可以將報告當成附件檢附？

A18:

漏洞掃描與滲透測試的部分，不論是公司內部的團隊進行測試或是委託第三方實驗室測試，需列出測試人員、進行測試的項目、測試狀況的架構以及使用的測試工具版本等資訊。其報告可當成附件檢附。

Q19:

請問「醫療器材網路安全評估分析參考範本」提到的漏洞掃描 Pass/Fail 的條件是可以自行定義的嗎？

A19:

可以，但是需要揭露 Pass/Fail 的標準並且應該符合科學邏輯。例如，標示“Pass”表示高風險是不存在的。

Q20:

請問「醫療器材網路安全評估分析參考範本」附錄一之醫療器材網路安全之業者揭露聲明書是否一定要按照表格勾選?

A20:

本次公布「醫療器材網路安全評估分析參考範本」附錄一之醫療器材網路安全之業者揭露聲明書(Manufacturer Disclosure Statement for Medical Device Security, MDS2)是參酌美國電子製造協會(National Electrical Manufacturers Association, NEMA)文件融合 IEC、NIST 等國際上針對醫療器材網路安全的相關規範，涵蓋各網路安全要項，有助業者盤點自家醫療器材產品網路安全情況並與國際調和，故建議按照表格逐項檢視勾選。

Q21:

請問「醫療器材網路安全評估分析參考範本」附錄一之醫療器材網路安全之業者揭露聲明書是軟硬體都有涵蓋嗎?

A21:

是，為符合醫療器材網路安全各樣態，醫療器材網路安全之業者揭露聲明書涵蓋軟硬體之範疇。

三、參考文獻

1. 109 年 1 月 15 日，醫療器材管理法。
2. 110 年 4 月 29 日，醫療器材許可證核發與登錄及年度申報準則。
3. 110 年 5 月 3 日，適用於製造業者之醫療器材網路安全指引。

4. 110 年 12 月 6 日，醫療器材網路安全評估分析參考範本。

醫療器材軟體上市後變更申請

常見問答集

111 年 3 月

一、前言

為協助業者瞭解我國醫療器材軟體上市後變更申請之管理，衛生福利部食品藥物管理署(下稱食藥署)特撰擬「醫療器材軟體上市後變更申請管理常見問答集」，以協助業者管理上市後醫療器材軟體產品之安全及有效性。惟本問答集未能全面涵蓋、解釋所有醫療器材軟體產品，業者應視產品軟體架構與設計之技術特點，評估產品發生之變化是否影響產品之安全及有效性，並依規定申請許可證變更，若無法確認，可準備相關資料向食藥署申請函詢，以確認產品是否須依《醫療器材許可證核發與登錄及年度申報準則》，向中央主管機關提出許可證變更之申請。

二、常見問答集

(一)業者應如何確認醫療器材軟體之變化情況是否需要申請許可證變更?

建議業者先自行評估醫療器材軟體產品之變化，若軟體自身變化調整或更新之累積效應或其軟體載具、所搭配之電腦主機、硬體週邊設備等之變更不影響醫療器材軟體本身之效能或用途，且不會影響其使用上之安全性及有效性，亦非屬《醫療器材許可證核發與登錄及年度申報準則》規定須申請許可證變更之項目，則無須申請許可證變更，惟其產品變化歷程結果及

相關之必要措施應製作紀錄並保存。

若屬《醫療器材許可證核發與登錄及年度申報準則》第 13 條所規範，或影響醫療器材軟體安全性及有效性之變更事項，則應依法申請許可證變更，經核准始得為之。

為協助業者瞭解醫療器材軟體上市後變更之相關管理規範，食藥署研擬《醫療器材軟體上市後變更申請之管理指引》，以作為業者申請許可證變更之參考，惟指引未能全面涵蓋、解釋所有醫療器材軟體產品，業者仍應視產品軟體架構與設計之技術特點，評估產品發生之變更是否影響其安全及有效性，並依規定申請許可證變更。

(二)醫療器材的韌體或行動應用程式(App)改變是否須申請許可證變更?

醫療器材的韌體或行動應用程式(App)改變若影響產品之安全及有效性(例如改變涉及須重新進行風險分析)，應依《醫療器材許可證核發與登錄及年度申報準則》規定辦理許可證變更，以確保產品之安全及有效性。另可參考食藥署公布之《醫療器材軟體上市後變更申請之管理指引》，其適用範圍為已取得許可證之醫療器材軟體產品，包含但不限於醫療器材之韌體或行動應用程式等。

(三)新增連線功能或從有線變為無線傳輸，是否需要申請變更?

醫療器材新增連線功能或從有線變為無線傳輸為規格之改變，可能影響產品之安全及有效性，如網路安全(Cybersecurity)，須依《醫療器材許可證核發與登錄及年度申報準則》規定，申請許可證變更。

(四)若產品之操作介面配合使用者要求新增輸入參數或備註的欄位功能等，是否需要申請許可證變更？

建議可先確認醫材軟體操作介面可新增欄位或功能是否為原核准產品之既有功能，若否，則建議先評估醫材軟體操作介面新增欄位或功能是否影響產品實際操作之安全及有效性，若有影響，建議依規定申請許可證變更。

(五)利用機器學習技術的人工智慧醫療器材之資料集（Dataset）有不斷變動之特性，是否需每隔一段時間即申請許可證變更？

人工智慧/機器學習技術的產品之資料可區分為訓練用、驗證用及測試用資料，當改變訓練用或驗證用資料集而影響到產品之安全性和有效性，須依規定申請許可證變更，若有疑慮也可以向本署提出函詢。

(六)利用機器學習技術的產品之模型，在不影響到產品之安全性和有效性的狀況下，可以修正軟體錯誤(debug)嗎?

若修正軟體錯誤未涉及改變原核准產品實際使用之安全及有效性，且未改變產品原核准範圍(如規格、效能等)，尚符合業者對於產品之品管維護，得無須辦理變更，但製造業者應對於相關修正保留完整變更紀錄。

(七)當醫療器材軟體需搭配之醫療器材(如電腦斷層掃描、磁振造影等儀器)之硬體設備或韌體改變時，醫療器材軟體是否需要申請許可證變更？

當醫療器材軟體搭配之醫療器材之硬體、韌體改變時，建議先評估是否影響醫療器材軟體之安全及有效性，例如產品若是針對某特定廠牌醫療器材輸出之資料(如醫學影像、數據等)進行醫材軟體架構之建置、模型訓練等，當市面上該廠牌儀器之硬體設備或韌體發生改變，可能影響產品原核准功能之表現，建議準備相關佐證資料，向本署申請許可證變更。

(八)若改變醫療器材軟體適用之作業系統，是否需要申請許可證變更？

當醫療器材軟體適用之作業系統版本升級（如由 Windows 7

升級為 Windows 10）或更換（如由 Windows 改變為 iOS)時，可能影響產品之系統相容性及功能，為確認作業系統版本改變後之產品功能與原核准一致，故建議準備前述佐證資料，依規定申請許可證變更，以確保產品之安全及有效性。

三、參考資料

(一) 109 年 1 月 15 日，《醫療器材管理法》。

(二) 110 年 4 月 29 日，《醫療器材許可證核發與登錄及年度申報準則》。

(三) 110 年 8 月 16 日，《人工智慧/機器學習技術之醫療器材軟體查驗登記技術指引》。

(四) 110 年 12 月 30 日，《醫療器材軟體上市後變更申請之管理指引》。