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。