
醫療器械行政管理制度

醫療器械軟件及網絡安全

技術參考文件：**TR-007**



中華人民共和國
香港特別行政區政府衛生署

Department of Health

The Government of the Hong Kong Special Administrative Region

The People's Republic of China

修訂記錄

版本	修訂日期	修訂摘要	參考編號
0	2025年9月1日	<ul style="list-style-type: none">首次於2025 年 9月發表的版本名為《醫療器械軟件及網絡安全》（第TR-007號技術參考文件）(中文版)	TR-007:2025(C)

目錄

1.	引言	4
2.	範圍	4
3.	定義及縮寫	5
4.	醫療器械軟件	6
5.	醫療器械行政管理制度中的醫療器械軟件表列	7
6.	醫療器械軟件的改動	13
7.	查詢	14
8.	參考資料	14

1. 引言

1.1 背景

- 1.1.1 在現有的框架下，醫療器械行政管理制度（MDACS）於《醫療器械安全及性能基本原則》中，針對以下兩類醫療器械軟件所涉及的公眾健康風險進行管制，包括醫療器械(MD)中的嵌入的軟件，即醫療器械軟件組件（SiMD），和獨立運作的醫療器械軟件，即醫療器械獨立軟件（SaMD）。隨著科技的發展及全球對醫療器械的管制趨勢變化，需要對軟件組件和獨立軟件的管理，尤其是後者，進行更新和詳細闡述，以尋求在保護病人/消費者安全與促進創新之間取得平衡。
- 1.1.2 醫療器械的數字化和無線連接提升了器械的性能和醫療服務的效率。然而，這可能因網絡的應用而暴露系統漏洞，帶來潛在風險。網絡安全威脅已經成為醫療器械製造商在開發軟件過程中的重要考量，以保護病人數據和臨床服務不會因網絡漏洞而遭受攻擊。
- 1.1.3 本文件旨在提供：
- (a) 為醫療目的而開發的軟件的概述；(b) 醫療器械行政管理制度框架下對醫療器械軟件的分級概念和分級原則；及
 - (c) 在醫療器械行政管理制度下對醫療器械網絡安全的基本要求。

2. 範圍

2.1 本文件重點闡述醫療器械軟件的概述和定義。

2.2 本文件旨在提供以下定義：

2.2.1 當軟件是嵌入在醫療器械中，即醫療器械軟件組件，及

2.2.2 當獨立運作的軟件被視為醫療器械，即醫療器械獨立軟件。

2.3 本文件亦根據醫療器械行政管理制度中的要求，提供與醫療器械軟件相關的表列指引，包括分級規則和網絡安全要求。

3. 定義及縮寫

3.1 **醫療器械獨立軟件(SaMD)**，是指旨在用於一個或多個醫療用途的軟件，無須作為醫療器械硬件其一部分亦可實現該醫療用途。

註：

(a) 醫療器械獨立軟件被視為一種醫療器械(MD)，包括一般醫療器械(GMD)和體外診斷醫療器械(IVDMD)。

(b) 醫療器械獨立軟件可以在一般用途（非醫療用途）的計算平台上運行，包括硬件和軟件資源（例如操作系統、處理硬件、儲存、軟件庫、顯示器、輸入設備、程式編製語言等）。

(c) 「無須作為其一部分」，意指不需要醫療器械硬件也能達到自身原擬醫療用途的軟件。

(d) 如軟件的原擬目的是驅動醫療器械硬件，則不符合醫療器械獨立軟件的定義。

(e) 醫療器械獨立軟件可以與其他產品（例如以組件模式），包括醫療器械，結合使用。

(f) 醫療器械獨立軟件可以與其他醫療器械，包括醫療器械硬件、其他醫療器械獨立軟件和通用軟件進行對接。

(g) 符合上述定義的流動應用程式可被視為獨立軟件。

(h) 醫療器械獨立軟件亦可：

- 提供疾病緩解的方法和建議；或
- 提供有關相容性測試、檢測、診斷、監測或治療生理狀況、健康狀況、疾病或

先天性畸形的資料；或

- 輔助診斷、篩查、監測、釐定易感性、預知、預測和釐定生理狀況。

3.2 **醫療器械軟件組件(SiMD)**，是指旨在用於一個或多個醫療用途的軟件，通過控制和操作醫療器械硬件或運行於醫用計算平台以實現該醫療用途。

3.3 本文件內所用術語的定義及縮寫，請參閱《醫療器械行政管理制度中的定義及縮寫》(指南第 GN-00 號)。

4. 醫療器械軟件

4.1 醫用軟件包括醫療器械軟件組件和醫療器械獨立軟件。

4.1.1 **醫療器械軟件組件(SiMD)**，是指旨在用於一個或多個醫療用途的軟件，通過控制和操作醫療器械硬件或運行於醫用計算平台以實現該醫療用途。例子：

(a) 擬用於操作臨床化學分析儀的軟件。

(b) 嵌入在心電圖(ECG)器械中的軟件，擬用於控制該器械以獲取病人的心電圖數據並打印結果。

4.1.2 **醫療器械獨立軟件(SaMD)**，是指旨在用於一個或多個醫療用途的軟件，無須作為醫療器械硬件其一部分亦可實現該醫療用途。

4.1.3 醫療器械獨立軟件亦可：

(a) 提供疾病緩解的方法和建議；或

(b) 提供有關相容性測試、檢測、診斷、監測或治療生理狀況、健康狀況、疾病或先天性畸形的資料；或

(c) 輔助診斷、篩查、監測、釐定易感性、預知、預測和釐定生理狀況。

4.1.4 以下是醫療器械獨立軟件的例子：

- (a) 用作分析心律數據，並輔助醫療人員診斷心律不正的軟件。
- (b) 進行數據插值來提供對病人的電腦斷層掃描影像的三維重建，使肺組織內的支氣管樹結構變得可視化，以協助置入導管及放置標記物，從而指導放射手術及胸腔手術的軟件。
- (c) 利用智能電話內的話筒來偵測睡眠期間的呼吸中斷，並發出提示音喚醒睡眠者的軟件。
- (d) 針對微創治療干預有效的情況下，擬在提供聲音療法來治療、緩解或減輕耳鳴影響的軟件。

4.1.5 醫療用途的軟件亦包括人工智能醫療器械，其附加表列要求，請參閱技術參考文件第TR-008號《人工醫療器械》。

5. 醫療器械行政管理制度中的醫療器械軟件表列

5.1 根據醫療器械行政管理制度下，醫用軟件也被視為醫療器械。

5.2 醫療器械軟件的分級須根據技術參考文件第TR-003號《一般醫療器械分級》和第TR-006號《體外診斷醫療器械分級》之風險分級原則。

5.2.1 醫療器械軟件組件通常是作為醫療器械硬件的組件/配件並結合使用，其分級應根據整個器械組合的原擬用途來分級。申請人宜將此軟件與相關的醫療器械硬件一併表列。申請人如欲獨立表列醫療器械軟件組件，則須於表列申請中提供充分理由，詳細說明獨立表列該軟件組件的必要性，並明確聲明相關的醫療器械硬件是否將納入醫療器械行政管理制度中的進行表列。此類申請須經由醫療器械科(MDD)的批准方可獲得表列。

5.2.2 醫療器械獨立軟件通常是獨立運作及無須與醫療器械硬件配合使用。一般情況下，獨立軟件應單獨表列，並根據技術參考文件第TR-003號和第TR-006號之分級規則進行分級。

5.3 適用的分級規則

5.3.1 根據醫療器械行政管理制度下的分級規則，醫療器械軟件被視作為有源醫療器械。

5.3.2 對於醫療器械軟件組件，該軟件是嵌入/安裝在醫療器械硬件內以執行特定醫療用途，通常應與醫療器械硬件一併表列。如需獨立表列/分級，應參考以下規則：

(a) 規則 11 可適用於：當軟件能夠控制或影響醫療器械硬件，以將藥物製品、體液或其他物質輸入身體及／或將之從身體移除。

(b) 規則 12 適用於不直接控制任何醫療器械硬件，或不以獨立方式提供任何醫療用途的軟件。例子：臨床資料傳輸和僅用作於顯示醫療影像等。此類器械並不屬於醫療器械行政管理制度中的表列範圍內。

5.3.3 對於醫療器械獨立軟件，如該原擬用途分別與治療和診斷目的相關，則適用於規則 9 和規則 10。

5.4 提交的技術文件須包括但不限於以下要素：

5.4.1 已認可的品質管理系統(QMS)

5.4.1.1 所有醫療器械製造商應具備已認可的品質管理系統，以確保醫療器械的製造質量，包括醫療器械軟件在內。ISO 13485 《醫療器械 — 質量管理體系 — 用於法規的要求》標準或同等標準，已指定和闡述品質管理系統的要求，醫療器械製造商可以在醫療器械的生命周期過程中採用相關標準。

5.4.1.2 製造商須設有品質管理系統，並註明該系統是屬於完整還是部分品質管理系統。如為部分品質管理系統，則須註明所涵蓋的程序範圍和品質管理系統核證的機構。

5.4.2 醫療器械安全及性能基本原則（技術參考文件第TR-004號）。

5.4.2.1 所有醫療器械，包括軟件，的安全及性能，均須符合國際標準。醫療器械行政管理制度中的「符合基本原則核對表」(表格MD-CLL或IVDMD-CCL)已表明醫療器械的基本設計和生產要求。特定醫療器械的相關要求亦須被識別。如該器械並無適用要求，該原因則須妥善記錄和以書面留檔。

5.4.2.2 製造商須了解技術參考文件第TR-004號之全面檢查表要求。如任何在指南第GN-02號提及的市場銷售核准在2004年12月31日或之前獲得，則須應要求提交「符合基本原則核對表」。否則，則須夾附已填妥的「符合基本原則核對表」。

5.4.2.3 或者，如申請人如能提供已按照歐盟的醫療器械相關指令或規例備妥「基本規定核對表」(Essential Requirements Checklist) 或「一般安全和性能要求核對表」(General Safety and Performance Requirements Checklist)，及有足夠證明顯示該產品亦同時符合醫療器械行政管理制度所訂的規定，申請人可選擇提交該「基本規定核對表」(Essential Requirements Checklist) 另附加「符合基本原則聲明」。

5.4.3 標籤要求

5.4.3.1 器械標籤（實體標籤、使用說明、使用手冊等）是使用者用作識別器械的重要資料，以便相關人士有效地傳達安全及性能的相關事宜。它亦有助於確保器械的可追溯性。為了正確識別某醫療器械軟件，製造商應在器械標籤上提供器械型號、產品代碼和軟件版本等資料。

5.4.3.2 申請人須提交所有標籤，包括說明、手冊、器械和包裝標籤（按照技術參考文件第TR-005號《醫療器械標籤附加規定》所註明），及「特別表列資料」（按照指南第GN-01號《醫療器械行政管理制度概覽》所註明）。不過，由於醫療器械獨立軟件可能不存在實體產品，只能從互聯網下載，製造商須向使用者提供獲取器械標籤的方式，例如從網站下載的電子版使用說明。申請人亦須提供相關的網站，並在表列申請時提交及證明獲取標籤的過程，例如提供相關使用說明網站的截圖。

5.4.4 風險管理

醫療器械軟件的風險管理至關重要，以便識別和減輕所有在整個器械使用壽命內可預見的安全及性能相關的風險。根據潛在風險的嚴重性和發生頻率，製造商須在實際可行的範圍內採取相應的補救措施，並評估其有效性。製造商應參考ISO 14971 《醫療器械 - 風險管理在醫療器械中的應用》或同等標準所規定的準則。對於包含網絡應用的醫療器械軟件，製造商亦須遵循本文件關於網絡安全的要求。

5.4.5 臨床評估

5.4.5.1 臨床評估意指對有關的科學文獻的系統性審查，及／或對臨床研究收集所得的數據進行分析和評估（請參照指南第 GN-00 號所載關於臨床研究的定義）。這個過程旨在確定器械符合技術參考文件第TR-004中相關的基本原則，並證明器械性能與製造商的原擬設計一致。臨床評估確立當與器械的效益一起衡量時，器械的風險及副作用是否可以接受。臨床評估及其結果均須載於臨床評估報告內。

5.4.6 醫療器械行政管理制度認可的市場銷售核准。

5.4.6.1 申請人須提供指南第GN-02號或指南第GN-06號所述的司法管轄區的市場銷售核准。

以下表格對醫療器械科的出版文件，以及與之對應技術文件相關的認可標準（或同等標準）作出簡述。

	醫療器械科的出版文件 / 認可標準
已設立的品質管理系統	ISO 13485 《醫療器械 — 質量管理體系 — 用於法規的要求》 GB/T 42061 《醫療器械 — 質量管理體系 — 用於法規的要求》
醫療器械安全及性能基本原則和相關指南	指南第GN-02號：《第II/III/IV級一般醫療器械表列指南》 指南第GN-06號：《第B，C及D級體外診斷醫療器械表列指南指南》 技術參考文件第TR-004號：《醫療器械安全及性能基本原則》
標籤規定	指南第GN-01號：《醫療器械行政管理制度概覽》 技術參考文件第TR-005號：《醫療器械標籤附加規定》

	ISO 15223-1 《醫療器械 — 用於醫療器械標籤、標記和提供資訊的符號 — 第1部分：通用要求》
風險管理	ISO 14971 《醫療器械 — 風險管理對醫療器械的應用》
臨床評估	ISO 14155 《醫療器械用於臨床受試者之臨床研究 — 良好臨床規範》
醫療器械行政管理制度中認可的市場銷售核准	指南第GN-02號：《第II/III/IV級一般醫療器械表列指南》 指南第GN-06號：《第B，C及D級體外診斷醫療器械表列指南》

有關一般醫療器械和體外診斷醫療器械的詳細表列要求，請分別參閱指南第GN-02號和指南第GN-06號。

5.5 醫療器械軟件的表列還需要一些特定文件要求，其中包括但不限於：

- (a) 軟件驗證及確認；
- (b) 軟件版本控制及可追溯性；及
- (c) 器械涉及無線或網絡傳輸的網絡安全管理。

5.5.1 軟件的驗證及確認

5.5.1.1 除了臨床研究外，驗證及確認都是證明軟件的安全有效性，以及證明其聲稱的原擬用途的重要流程。

5.5.1.2 在一般軟件的開發生命週期，驗證旨在確保軟件規格能從預設的數據輸入提供預期的結果，亦允許製造商確保軟件的設計符合其規格。另一方面，確認旨在提供證據以證明該軟件的開發符合原擬用途和使用者需求。

5.5.1.3 申請人可以參閱國際標準，例如 IEC 62304《醫療器械軟件 — 軟件生命週期過程》或同等標準，以證明器械符合其要求。

5.5.2 軟件版本控制及可追溯性

5.5.2.1 軟件版本控制對推出市場後事件（例如醫療事件、產品投訴或安全警示等）的追蹤尤為重要。申請人須確保所表列的軟件與已提交的技術文件版本相等。此外，請儘可能在市場銷售核准文件中清楚識別軟件版本。

5.5.2.2 如軟件有任何版本更新，本地負責人(LRP)須根據指南第GN-10號《表列醫療器械的改動指南》之要求提交改動申請。

5.5.3 醫療器械的網絡安全

5.5.3.1 現時，醫療器械傾向通過無線連接或網絡（例如互聯網）進行互聯。這可能會帶來風險，例如在網絡連接的器械進行數據傳輸時洩露病人資料。因此，在整個產品生命週期中，須考慮和實施必要的資訊保安措施和保護，以防止在網絡漏洞遭受攻擊。

5.5.3.2 製造商須儘可能識別和減輕可預見的網絡安全風險。製造商亦有責任評估和管理任何危害病人、使用者或其他人健康和安全的網絡安全風險。如應用產品包含任何醫療器械軟件，製造商需要在醫療器械的使用壽命內處理有關網絡安全風險，包括但不限於：

- (a) 一般考慮因素，例如開發方法、管理常規、標準應用、風險管理策略、基礎設施、製造和供應鏈管理，以及為使用者提供的資料；
- (b) 技術考慮因素，例如網絡安全滲透測試、模組化設計架構、操作平台安全性、新興軟件及信任存取和內容提供；
- (c) 器械原擬用途的環境考慮因素，例如網絡連接、上傳或下載數據；
- (d) 實體考慮因素，例如器械及界面上的機械鎖、物理網絡安全和廢物管理（防止泄露敏感紙本信息）；及
- (e) 社會考慮因素，例如消除或減少社會-工程威脅（例如網絡釣魚、冒充、誘騙和尾隨）。

5.5.4 基本網絡安全要求

5.5.4.1 符合醫療器械行政管理制度之基本網絡安全要求的醫療器械軟件，可代表製造商已經：

- (a) 將網絡安全風險和漏洞視為醫療器械整個使用壽命內全面風險管理的一部分。
- (b) 採取措施避免使用普遍默認密碼。使用密碼時，每台醫療器械的密碼須為獨特或由使用者自行更改。使用預設密碼時，每台器械的密碼須為獨特和具有足夠的隨機性。此外，醫療器械須配備一種機制，使對其身份驗證機制的暴力破解攻擊變得不可行。
- (c) 建立漏洞披露系統以管理漏洞呈報。
- (d) 制定持續的計劃，以主動監測、識別和修復新發現的漏洞，並確保醫療器械在整個使用壽命內的性能及安全性。

5.5.5 技術文件須涵蓋上述考慮因素和要求，包括風險管理報告及其他補充文件。由於網絡安全風險可能影響醫療器械的安全性，相關風險的評估和緩解措施必須符合醫療器械行政管理制度中的基本原則的規定，並反映在風險管理過程中。

5.5.6 申請人可以參閱有關標準或同等標準，例如但不限於：

- (a) ISO 27032 《網路安全 — 互聯網安全指南》
- (b) ISO/IEC 27001 《資訊安全、網路安全與隱私保護 — 資訊安全管理體系》

5.5.7 申請人須注意並遵循中華人民共和國香港特別行政區政府數字政策辦公室發出的相關網絡安全良好實務、要求或建議（如適用）。

6. 醫療器械軟件的改動

6.1 製造商和本地負責人須評估該改動對醫療器械軟件的功能、原擬用途、基本設計和對醫療器械軟件的製造特性及其分級（包括醫療器械軟件與其他醫療器械組合的分級）所造成的潛在影響。如軟件的功能或原擬用途受到影響，則須進行適當的風險評估，並在風險管理報告加以說明。製造商亦須在軟件推出市場使用前，進行適當的確認及驗證。

6.2 有關申請改動的程序和要求，請參閱指南第GN-10號。

7. 查詢

7.1 如對本文件及醫療器械行政管理制度有疑問，請按下述聯絡方法提出查詢：

衛生署

衛生署醫療器械科

電話號碼：3107 8484

傳真號碼：3157 1286

電郵地址：mdd@dh.gov.hk

網頁：www.mdd.gov.hk

7.2 與醫療器械行政管理制度有關的指南及表列申請表可於網站 <https://www.mdd.gov.hk> 下載。

8. 參考資料

8.1 國際醫療器械監管機構論壇《醫療器械獨立軟件：核心定義》

8.2 國際醫療器械監管機構論壇《醫療器械獨立軟件：風險分類框架及相應考量》（第 SaMD WG N12號）

8.3 國際醫療器械監管機構論壇《醫療器械獨立軟件：品質管制體系應用》

8.4 國際醫療器械監管機構論壇《醫療器械獨立軟件：臨床評估》

8.5 衛生署《醫療器械行政管理制度中的定義及縮寫指南》（第 GN-00 號指南）

8.6 衛生署《醫療器械行政管理制度概覽指南》（第GN-01號指南）

8.7 衛生署《第 II/III/IV 級一般醫療器械表列指南》（第 GN-02 號指南）

8.8 衛生署《第 B, C 及 D 級體外診斷醫療器械表列指南》（第 GN-06 號指南）

8.9 衛生署《表列醫療器械的改動指南》（第 GN-10 號指南）

8.10 衛生署《一般醫療器械分級》（第 TR-003 號技術參考文件）

8.11 衛生署《醫療器械安全及性能基本原則》（第 TR-004 號技術參考文件）

- 8.12 衛生署《體外診斷醫療器械分級》（第 TR-006 號技術參考文件）
- 8.13 國際標準組織 ISO 13485:2016 《醫療器械 — 質量管理體系 — 用於法規的要求》
- 8.14 國際標準組織 ISO 14971:2019 《醫療器械 — 風險管理在醫療器械中的應用》
- 8.15 國際標準組織 ISO 14155:2020 《醫療器械用於臨床受試者之臨床研究 – 良好臨床規範》
- 8.16 國際標準組織 ISO 15223-1:2021 《醫療器械 — 用於醫療器械標籤、標記和提供資訊的符號 — 第1部分：通用要求》
- 8.17 國際電工委員會 IEC 62304:2006 《醫療器械軟件 — 軟件生命週期過程》
- 8.18 國際標準組織 ISO 27032:2012 《網路安全 — 互聯網安全指南》
- 8.19 國際標準組織/國際電工委員會 ISO/IEC 27001:2022 《資訊安全、網路安全與隱私保護 — 資訊安全管理體系》
- 8.20 新加坡衛生科學局 《軟體醫療器械監管指南 — 生命週期管理方法》 第2.0版 2022年4月
- 8.21 新加坡網路安全局 《醫療器械網路安全標籤計畫》 技術規範第2號檔 第0.5版 2023年10月
- 8.22 Therapeutic Goods Administration. Medical device cyber security guidance for industry.
- 8.23 國家藥品監督管理局《醫療器械軟件注冊技術審查指導原則》
- 8.24 國家藥品監督管理局《醫療器械網路安全注冊技術審查指導原則》
- 8.25 歐盟醫療器械協調小組 《歐盟第 (EU) 2017/745 編號和第 (EU) 2017/746 編號法規下軟件認定和分類指南》（第 MDCG 2019-11號文件）
- 8.26 歐盟醫療器械協調小組 《醫療器械網路安全指南》（第 MDCG 2019-16 號文件）