第 21/ISAF/2026 號批示

藥物監督管理局局長行使第 12/2025 號法律《醫療器械監督管理制度》第四條第二款（四）項賦予的職權，並根據第 12/2025 號法律第三十三條第三款的規定，作出本批示。

一、核准《醫療器械獨立軟件生產質量管理規範》，該技術性指示載於作為本批示組成部分的附件。

二、因適用本批示而產生的疑問，由藥物監督管理局局長作出決定解決。

三、本批示自二零二六年七月一日起生效。

二零二六年六月十日於藥物監督管理局

局長 蔡炳祥

附件

（第一款所指者）

醫療器械獨立軟件生產質量管理規範

1. 適用範圍及原則

1.1. 本規範適用於屬醫療器械的獨立軟件（下稱“獨立軟件”），而軟件組件可參照適用。

1.2. 本規範遵循軟件生存周期過程及網絡安全的基本原則及通用要求，是對獨立軟件的生產質量管理規範的特殊要求，獨立軟件的生產質量管理體系須符合經第16/ISAF/2026號批示核准的《醫療器械生產質量管理規範》及本規範的要求。對本規範未有規定的事宜，補充適用《醫療器械生產質量管理規範》。

2. 人員

2.1. 獨立軟件的開發、測試及維護人員須具備與崗位職責要求相適宜的專業知識、實踐經驗及工作能力。

2.2. 黑盒測試須保證同一獨立軟件項的開發人員不得兼任測試人員，反之亦然。

2.3. 用戶測試人員須具備適當的獨立軟件使用經驗，或經過培訓具備適當的使用相關獨立軟件的技能。

3. 設備

3.1. 在獨立軟件生存周期過程中，醫療器械製造准照持有人（下稱“製造商”）須持續提供充分、適當及有效的獨立軟件開發及測試環境，尤其包括軟硬件設備、開發測試工具及網絡等資源，以及病毒防護、數據備份與恢復等保證措施。

3.2. 製造商須制定獨立軟件開發及測試環境維護的規定並形成文件，以明確對獨立軟件開發及測試環境進行定期驗證、更新升級及病毒防護等活動的要求，並保存相關紀錄。

4. 設計開發

4.1. 製造商須結合獨立軟件生存周期模型特點，建立獨立軟件生存周期過程的控制程序並形成文件，該控制程序須就獨立軟件的開發策劃、需求分

析、設計、編碼、驗證與確認、更新、風險管理、缺陷管理、可追溯性分析、配置管理、文件與紀錄控制、現成軟件使用、網絡安全、發佈、部署及停運等活動制定要求。

4.2. 在獨立軟件生存周期過程中，對獨立軟件質量保證活動的要求須與其安全性級別相適宜。在採取風險控制措施之前，製造商須根據獨立軟件的預期用途、使用場景及核心功能，綜合判定其安全性級別，且僅可通過外部風險控制措施降低該安全性級別。

4.3. 製造商須根據風險管理控制程序實施獨立軟件的風險管理活動，該控制程序須包含對獨立軟件的功能、接口、用戶界面、現成軟件及網路安全等風險的識別、分析、評價、控制及監測，並貫穿於獨立軟件的整個生存周期。

4.4. 製造商須對獨立軟件配置管理建立控制程序並形成文件，該控制程序須規範獨立軟件版本、源代碼、文件、工具及現成軟件等控制要求，確定配置標識、變更控制及配置狀態紀錄等活動要求，並於獨立軟件的整個生存周期使用配置管理工具，以確保獨立軟件質量。

4.5. 製造商須根據合規性的要求建立獨立軟件版本控制的命名規則，涵蓋獨立軟件、現成軟件及網絡安全的全部軟件的更新類型，各字段含義須明確、無歧義及無矛盾。獨立軟件版本的變更亦須符合該獨立軟件版本命名規則的要求。

4.6. 製造商須對獨立軟件可追溯性分析建立控制程序並形成文件，涵蓋現成軟件及網絡安全的控制要求，形成軟件可追溯性分析報告以供評審，並於獨立軟件的整個生存周期使用可追溯性分析工具，以確保獨立軟件開發及其更新過程滿足可追溯性要求。

4.7. 製造商須對現成軟件的使用形成文件，制定風險管理、驗證與確認、缺陷管理、可追溯性分析、軟件更新、配置管理、文件與紀錄控制及網絡安全等活動的要求。遺留軟件還須制定現有文件、上市後使用情況、用戶投訴、不良事件及回收情況等評估活動要求。使用開源軟件須遵循相應的開源許可協議。

4.8. 製造商須就獨立軟件的開發策劃制定需求分析、設計、編碼、驗證與確認、風險管理、缺陷管理、可追溯性分析、配置管理、文件與紀錄控制、現成軟件使用、網絡安全及評審等活動計劃，形成相關文件並適時更新，以及保存相關活動紀錄。獨立軟件開發策劃須確保獨立軟件開發、測試的人員及測試環境均與獨立軟件的開發要求相適宜。

4.9. 對於獨立軟件需求分析，製造商須綜合分析法律法規、標準、用戶、產品、功能、性能、接口、用戶界面、網絡安全及警示提示等需求，制定風險管理、可追溯性分析、現成軟件使用評估、軟件確認測試計劃創建

以及評審等活動要求，並形成獨立軟件需求規範及評審紀錄。該等規範及評審紀錄須獲得批准及適時更新，其更新亦須獲得批准。可追溯性分析則須分析獨立軟件需求與風險管理的關係、獨立軟件需求與產品需求的關係。

4.10. 對於獨立軟件的設計，製造商須根據獨立軟件需求規範實施軟件體系架構、功能、性能、算法、接口、用戶界面、單元及網絡安全等設計，制定風險管理、可追溯性分析、現成軟件使用評估、軟件驗證測試計劃創建以及評審等活動要求，並形成獨立軟件設計規範及評審紀錄。該等規範及評審紀錄須獲得批准及適時更新，其更新亦須獲得批准。可追溯性分析則須分析獨立軟件設計與獨立軟件需求之間的關係。

4.11. 製造商須根據獨立軟件設計規範實施軟件編碼，制定源代碼編寫與註釋、現成軟件使用、可追溯性分析、各級測試用例創建及評審等活動要求，形成評審紀錄及適時更新。源代碼的編寫及註釋須符合軟件編碼規則文件的要求。測試用例須確保充分、適宜及有效地進行獨立軟件的驗證與確認測試。可追溯性分析則須分析源代碼與獨立軟件設計的關係，以及源代碼與測試用例的關係。

4.12. 製造商須就軟件驗證制定源代碼審核、靜態分析、動態分析、單元測試、集成測試、系統測試及評審等活動要求，涵蓋對現成軟件及網絡安全的驗證要求，並保存相關紀錄。還須就白盒測試制定語句、判定、條件及路徑等測試覆蓋率要求，且該等要求須與軟件安全性級別相適宜。

4.13. 製造商須根據相應的測試計劃進行單元測試、集成測試及系統測試，涵蓋對現成軟件及網絡安全的測試要求，並制定缺陷管理、風險管理、可追溯性分析及評審等活動要求，形成相應獨立軟件測試紀錄、測試報告以及評審紀錄，並適時更新。可追溯性分析則須分析各級測試用例與獨立軟件設計的關係、系統測試與獨立軟件需求的關係，以及系統測試與風險管理的關係。

4.14. 製造商須就軟件確認制定用戶測試、臨床評價及評審等活動要求，涵蓋對現成軟件及網絡安全的確認要求，並保存相關紀錄，確保獨立軟件滿足用戶需求及預期目的，且獨立軟件已知剩餘缺陷的風險均可接受。

4.15. 製造商須根據用戶測試計劃在真實使用環境或模擬使用環境下進行用戶測試，涵蓋對現成軟件及網絡安全的測試要求，並制定缺陷管理、風險管理、可追溯性分析及評審等活動要求，形成用戶測試紀錄、測試報告以及評審紀錄。該等報告及紀錄須獲得批准及適時更新，其更新亦須獲得批准。可追溯性分析則須分析用戶測試與用戶需求的關係，以及用戶測試與風險管理的關係。

4.16. 製造商須對獨立軟件更新形成文件，涵蓋對現成軟件及網絡安全的變更控制要求，並制定更新請求的評估、更新策劃、更新實施、風險管理、

驗證與確認、缺陷管理、可追溯性分析、配置管理、文件與紀錄控制、評審及用戶告知等活動要求，形成相關文件及紀錄。該等文件及紀錄須獲得批准及適時更新，其更新亦須獲得批准。軟件版本的變更須與軟件更新的情況相匹配。驗證與確認須根據軟件更新的類型、內容及程度實施相適宜的回歸測試及用戶測試等活動。

4.17. 製造商須對獨立軟件缺陷管理形成文件，制定缺陷評估、缺陷修復、回歸測試、風險管理、配置管理及評審等活動的要求，形成獨立軟件缺陷分析報告以供評審，並於獨立軟件的整個生存周期使用缺陷管理工具，以確保獨立軟件的質量。

5. 採購

5.1. 製造商須對現成軟件的採購形成文件。根據現成軟件的類型、使用方式及對獨立軟件的質量影響程度，制定分類管理、質量控制及供應商審核等活動要求。

5.2. 製造商須與供應商簽訂外包軟件質量協議，制定外包軟件的需求分析、交付形式、驗收方式與準則、設計開發文件交付、知識產權歸屬及維護等要求，以及雙方承擔質量責任的規定。

5.3. 如簽署雲計算服務的協議，其內須載明承擔網絡安全、患者數據與隱私保護等責任的規定。

6. 生產管理

6.1. 製造商須對獨立軟件的發佈形成文件，制定獨立軟件的文件創建、獨立軟件與文件歸檔備份、獨立軟件版本識別與標記、交付形式評估與驗證及病毒防護等活動要求，以確保獨立軟件發佈的可重複性。

6.2. 製造商須就獨立軟件的物理交付方式制定獨立軟件的複製、許可授權以及存儲媒介包裝、標記及防護等要求；如以網絡方式進行交付，製造商須制定獨立軟件的標記、許可授權及網絡安全等要求。

7. 質量控制

製造商須對獨立軟件的放行形成文件，制定獨立軟件版本識別、安裝卸載測試、獨立軟件完整性檢查及放行批准等活動要求，並保存相關紀錄。

8. 銷售及售後服務

8.1. 製造商須對獨立軟件的部署形成文件，制定交付、安裝、設置、配置及用戶培訓等活動要求，並保存相關紀錄。

8.2. 製造商須對獨立軟件的停運形成文件，制定停運後的用戶服務、數據遷

移、患者數據與隱私保護以及用戶告知等活動要求，並保存相關紀錄。

9. 不良事件監測、分析及改進

9.1. 數據分析控制程序須包括獨立軟件缺陷及網絡安全事件的規定。

9.2. 製造商須對網絡安全事件的應急響應形成文件，制定網絡安全事件的風險管理、應急響應措施驗證、用戶告知及回收等活動要求，並保存相關紀錄。

10. 術語及其含義

為適用本規範的規定，下列術語的含義為：

1) “獨立軟件”：是指具有一個或多個醫療目的，無需醫療器械硬件即可完成自身預期目的且運行於通用計算平台的軟件。

2) “軟件組件”：是指具有一個或多個醫療目的，控制或驅動醫療器械硬件或運行於醫用計算平台的軟件。

3) “軟件安全性級別”：是指基於獨立軟件風險程度分為輕微、中等及嚴重，其中輕微即不可能產生傷害，中等即可能直接或間接產生輕微傷害，嚴重即可能直接或間接產生嚴重傷害或導致死亡。

4) “軟件驗證”：是指通過客觀證據足以認定獨立軟件開發或更新某一階段的輸出滿足輸入的要求。

5) “軟件確認”：是指通過客觀證據足以認定獨立軟件滿足用戶需求及預期目的。

6) “軟件可追溯性分析”：是指追蹤獨立軟件的需求、設計、源代碼、測試與風險管理之間的關係，以分析已識別關係是否正確、一致、完整及準確。

7) “軟件更新”：是指製造商在獨立軟件生存周期全過程對獨立軟件所做的任一修改，又稱“軟件變更”或“軟件維護”。

8) “停運”：是指在製造商在獨立軟件生存周期過程末期終止對獨立軟件的售後服務及銷售，又稱“退市”。

9) “現成軟件”：是指製造商沒有進行完整生存周期控制的獨立軟件，包括遺留軟件、製成品軟件及外包軟件。

10) “遺留軟件”：是指由製造商以往開發，但現時無法能得到足夠開發紀錄的獨立軟件。

11) “製成品軟件”：是指已開發的、通常可取得的、但製造商沒有進行完整生存周期控制的獨立軟件。

12) “外包軟件”：是指製造商委託第三方開發的獨立軟件。

13) “網絡安全”：是指為確保使用的資訊網絡及電腦系統正常運作，以及電腦數據資料的完整性、保密性及可用性而開展的長期性跨領域活動，尤其防止該等網絡、系統及數據資料因未經許可的行為而受到不利影響。