本期專欄

醫療器材軟體應用、驗證及確效

財團法人台灣商品檢測驗證中心／黃馨儀

前言

近年來軟體越來越普及，被大量應用於醫療器材輔助診斷系統、智慧醫療器材及遠端照護醫療器材。美國FDA於2019年提出Off The Shelf (OTS) Software Use in Medical Devices guidance中，說明現已有許多現成的軟體套用於醫療器材上，並強調醫療器材軟體生命週期之維護與控制的重要性。另外美國FDA於2020年研討會提出具備人工智慧(Artificial intelligence, AI)及機器學習(Machine Learning, ML)技術軟體，當應用於醫療保健過程所產生大量的數據中，可得出新的重要見解來改變醫療保健，但同時也要維持軟體安全性及有效性。所以大數據的時代的軟體應用使得於醫療器材更為先進，然而隨著新技術與應用也新增了產品風險與管理的挑戰，因此需更為重視安全性、有效性、軟體生命週期維護、文件紀錄、風險管理及驗證確效。

接下來將藉由本篇說明現今醫療器材軟體應用、法規及規範的要求、醫療器材軟體驗證及確效，以及其實際軟體生命週期所須備齊的文件，讓讀者能進一步的了解。

一、人工智慧和機器學習如何被應用於醫療器材軟體上

初期的電腦輔助診斷系統為臨床專家以人工定義或選取特徵，藉由這些特徵演算法利用機器學習進行像是邊緣形態、紋理特徵等等的特徵工程。至現今對於醫學影像的分析及輔助診斷，包括X光、超音波、CT及MRI影像的發展主流已轉向為應用深度學習(deep learning)的方法，讓人工智慧可以自行學習特徵並進行分類。例如卷積神經網路(Convolution Neural Network, CNN)為基礎的神經網路對於影像有很強的辨別能力，而對於有時序概念的如波形則可利用遞歸神經網路(Recurrent Neural Network, RNN)透過不同樣本(pattern)之間的關聯度來增加特徵擷取的強度或是長短期記憶模型(Long Short-Term Memory, LSTM)的神經網路進行學習訓練，而越來越多的神經網路

也持續研究開發達到更準確的判斷及分類運用於醫療輔助診斷器材上。

美國FDA日前也陸續通過了幾件聲稱以AI當核心的輔助診斷醫材，如2018年4月份通過的IDx-DR，其可在無眼科專科醫師的監督下獨立診斷患者是否產生糖尿病視網膜病變，其他的如心電圖是否有異常心律不整的狀況、檢測手腕骨折及腦出血等等也有相關AI產品通過並上市。此類軟體不但屬於醫療器材軟體涵蓋範疇且應更為重視安全性、有效性及軟體生命週期維護。

二、醫療器材軟體涵蓋範疇

台灣TFDA於2017年公告了醫療器材軟體確效指引，其參考FDA Guidance及IEC 62304:2006/Amd 1:2015界定醫療器材軟體適用範圍涵蓋韌體、單獨軟體、安裝於一般用途電腦之軟體、專屬硬體／軟體醫療器材、軟體或由軟體組成之醫療器材配件。

至於醫療器材軟體的風險等級分類可參照美國FDA於2015年所提出Guidance for the Content of Premarket submission for Software Contained in Medical Device該規範與國際標準IEC 62304:2006/Amd 1:2015大同小異。FDA將嚴重程度分為重大風險等級(Major)、中等風險等級(Moderate)及輕微風險等級(Minor)；而IEC 62304則將軟體風險等級由低至高分為Class A、Class B及Class C，此分類是藉由Assigning software safety classification flow chart 所定義醫療器材軟體風險等級，差異說明如下方（表1）。而根據不同軟體風險等級所需檢附文件內容也有所不

表1：醫療器材軟體風險等級差異說明及開發生命週期應檢附資料[1, 2, 4]

FDA Guidance for the Content of Premarket submission for Software Contained in Medical Device, 200	輕微風險等級(Minor)：醫療器材軟體故障或潛在設計缺陷不會引起病患或使用者受到任何傷害。	中等風險等幾級(Moderate)：醫療器材軟體故障或潛在的設計缺陷可能直接導致病人或使用者輕微傷害。	重大風險等級(Major)：醫療器材軟體故障或潛在的設計缺陷可能直接導致病人或使用者嚴重傷害。
IEC 62304:2006/Amd 1:2015	Class A：軟體系統可能會導致危害情況，不會導致不可接受的風險。	Class B：軟體系統可能導致危害情況，可能產生危害是非嚴重傷害。	Class C：軟體系統可能導致危害情況，可能產生的危害是死亡或嚴重傷害。
醫療器材軟體之風險(Level of Concern)/ software safety classification	所有等級皆應說明該醫療器材軟體風險等級之判定過程與結果。		
醫療器材軟體之描述(Software Description)	所有等級皆應說明該醫療器材軟體之功能與操作環境。		
醫療器材之危害分析(Device Hazard Analysis)	所有等級皆針對該醫療器材軟體、韌體及硬體或者軟體系統進行風險鑑別、風險分析、風險評估、風險控制及改善措施。		

表1：醫療器材軟體風險等級差異說明及開發生命週期應檢附資料[1, 2, 4]（續1）

FDA Guidance for the Content of Premarket submission for Software Contained in Medical Device, 200	輕微風險等級(Minor)：醫療器材軟體故障或潛在設計缺陷不會引起病患或使用者受到任何傷害。	中等風險等幾級(Moderate)：醫療器材軟體故障或潛在的設計缺陷可能直接導致病人或使用者輕微傷害。	重大風險等級(Major)：醫療器材軟體故障或潛在的設計缺陷可能直接導致病人或使用者嚴重傷害。
IEC 62304:2006/Amd 1:2015	Class A：軟體系統可能會導致危害情況，不會導致不可接受的風險。	Class B：軟體系統可能導致危害情況，可能產生危害是非嚴重傷害。	Class C：軟體系統可能導致危害情況，可能產生的危害是死亡或嚴重傷害。
醫療器材軟體之需求規格(Software Requirements Specification (SRS))	摘要說明醫療器材軟體之功能需求規格。	完整說明醫療器材軟體之要求規格。	
醫療器材軟體設計規格(Software Design Specification (SDS))	無須檢附	應說明醫療器材軟體設計規格。	
醫療器材軟體設計架構圖(Architecture Design Chart)	無須檢附	詳述說明醫療器材軟體之功能單元(Functional unit)與模組(software modules)，並包含狀態圖(state diagrams)及流程圖(flow charts)。	
追溯性分析(Traceability Analysis)	所有等級應檢附醫療器材軟體追溯分析文件，其應包含軟體需求規格(SRS)、軟體設計規格(SDS)、危害鑑別(identified hazards)、危害分析(hazards analysis)、查證／驗證(verification)與確效(validation)測試之追溯紀錄。		
醫療器材軟體開發環境(Software Development Environment Description)	無須檢附	應說明醫療器材軟體生命週期開發計畫摘要	應說明醫療器材軟體生命週期開發計畫要，包含開發過程產生的控制文件。檢附軟體開發過程之控制／基準文件(control/baseline documents)及軟體編碼標準(coding standards)之敘述。
驗證與確認文件(Verification and Validation Documentation)／驗證確效及測試報告(Software integration and integration testing)	應說明軟體功能測試計畫(plan)、測試合格判定準則及測試結果摘要	敘述與軟體單元(unit)、整合(integration)及系統層級之查證／驗證與確認，並涵蓋系統層級測試方法(protocol)、測試合格判定準則及測試結果。	
軟體組態管理與維護計畫(Software Configuration Management Plan and Maintenance Plan)	應說明軟體管理組織人員、軟體版本、軟體文件命名、軟體變更程序及軟體維護規劃。		

表1：醫療器材軟體風險等級差異說明及開發生命週期應檢附資料[1, 2, 4]（續2）

FDA Guidance for the Content of Premarket submission for Software Contained in Medical Device, 200	**輕微風險等級(Minor)：醫療器材軟體故障或潛在設計缺陷不會引起病患或使用者受到任何傷害。**	**中等風險等幾級(Moderate)：醫療器材軟體故障或潛在的設計缺陷可能直接導致病人或使用者輕微傷害。**	**重大風險等級(Major)：醫療器材軟體故障或潛在的設計缺陷可能直接導致病人或使用者嚴重傷害。**
IEC 62304:2006/Amd 1:2015	Class A： 軟體系統可能會導致危害情況，不會導致不可接受的風險。	Class B： 軟體系統可能導致危害情況，可能產生危害是非嚴重傷害。	Class C： 軟體系統可能導致危害情況，可能產生的危害是死亡或嚴重傷害。
醫療器材軟體修訂歷史紀錄(Revision Level History)	應檢附醫療器材軟體修訂之歷史紀錄，包含日期、版本編號、版本變更內容及最終發行版本。		
為解決的異常(Unresolved Anomalies (Bugs or Defects)	無須檢附	應檢附尚未解決的異常列表，該等未解決的異常對於產品安全及有效性之影響，包括人因工程等。	

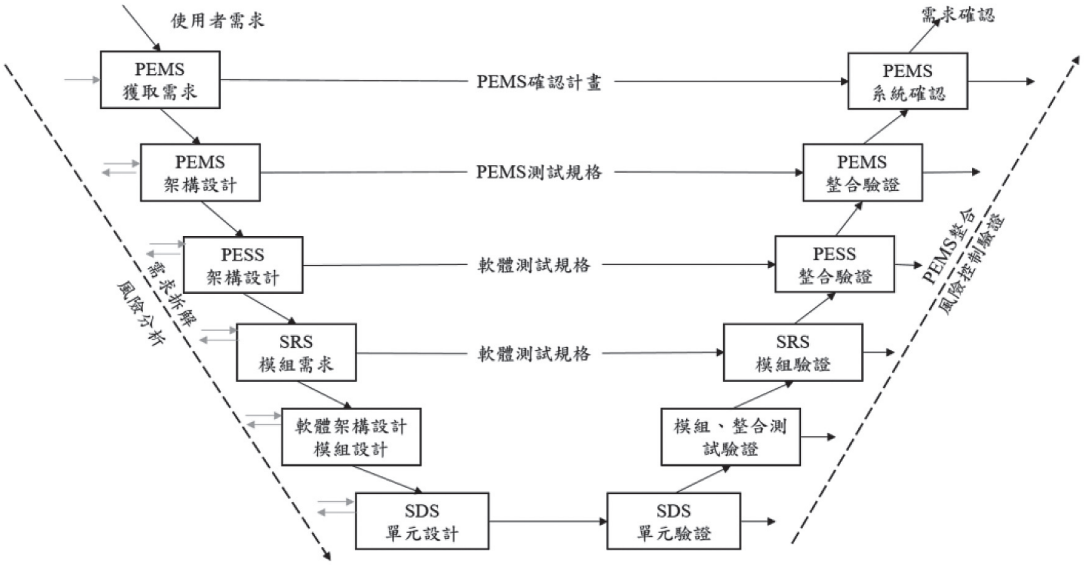

圖1：V模型軟體生命週期

同，當然隨著軟體風險等級越高則所需的文件就需越詳細。

三、醫療器材軟體生命週期涵蓋範圍

軟體確效是透過產品發展生命週期活動來評估軟體產品質的嚴謹方法。而產品軟體生命週期會因產品開發特性而套用不同開發模型，例如V模型、瀑布模型及螺旋模型等。以V開發模型舉例如（圖1），從使用者需求、可程式化電子醫療系統(Programmable Electrical Medical System, PEMS)、可程式化電子子系統(Programmable Electrical Subsystem,

PESS)、醫療器材軟體之需求規格、醫療器材軟體之設計規格及軟體設計單元，將其每個階段進行測試、驗證、確認至開發皆涵蓋在軟體軟體生命週期內。另外此生命週期也規範於IEC 60601-1:2005 +IEC 60601-1:2005/AMD1:2012第14章節中可與IEC 62304:2006/Amd 1:2015相互對應，其中截取法規相關章節的說明如（表2）。

四、軟體確效文件種類

（一）醫療器材軟體設計架構圖(Architecture Design Chart)

通常軟體設計架構圖會以流程方式說明醫療器材軟體中主要功能單元之間相互關係，包括軟體對於硬體和資料流(data flows)之關係[4]。

（二）醫療器材軟體需求規格(Software Requirements Specification (SRS))

醫療器材軟體需求規格包含功能、性能、介面、設計及開發等[4]，藉此份檔案規劃測試要求驗證方法的原則和定義，並說明滿足使用者需求及對臨床的重要性。

（三）醫療器材軟體設計規格(Software Design Specification (SDS))

醫療器材軟體設計規格描述該軟體如何實現軟體要求規格。就SRS和SDS之間的關係而言，SRS描述軟會做那些事，SDS描述如何實現SRS之要求[4]。亦是延伸SRS之需求細項擬定SDS並更深入建構設計軟體單元。

表2：IEC 60601-1:2005 +IEC 60601-1:2005/AMD1:2012與IEC 62304:2006/Amd 1:2015對照表[3]

PEMS requirements from IEC 60601-1:2005 +IEC 60601-1:2005/AMD1:2012	Requirements of IEC 62304 relating to the software subsystem of a PEMS
14.1 一般要求 1,14.2至14.12章節中的要求適用於可程式化電子醫療系統，除非可程式化電子子系統未提供基本安全或基本性能所需的功能，或者須於風險管理應用說明任何可程式化電子子系統不會導致不可接受的風險。 無論14.2至14.12中的要求是否適用，14.13章節可程式化電子醫療系統皆須評估IT-NETWORK(Information Technology Network)	4.3 軟體安全分類 IEC 60601-1的可程式化電子醫療系統大多要求適用於Class B和Class C，少部分要求適用於Class A。
14.2 檔案 此章節要求的文件應按照正式的文件程序進行審查、批准、發布和變更。	5.1 軟體開發計劃 軟體開發計劃中涉及的項目構成了軟體開發生命週期，其中涵蓋軟體驗證計劃、文件檔案規劃。
14.4 可程式化電子醫療系統開發生命週期 應記錄可程式化電子醫療系統開發生命週期每一個階段，應包含驗證方法、輸入、輸出、風險管理活動和文件檔案，並根據具體的發展情況量制定詳細的活動、項目和時間表。	

表2：IEC 60601-1:2005 +IEC 60601-1:2005/AMD1:2012與IEC 62304:2006/Amd 1:2015對照表[3]（續）

PEMS requirements from IEC 60601-1:2005 +IEC 60601-1:2005/AMD1:2012	Requirements of IEC 62304 relating to the software subsystem of a PEMS
14.5 問題解決 在適當的情況下，應制定和維護可程式化電子醫療系統開發生命週期的所有階段和活動之間和之間解決問題的文件化系統。	9 軟體問題解決過程
14.6 風險管理流程	7 軟體風險管理流程
14.6.1 識別已知和可預見的危害 製造商應鑑別與可程式化電子醫療系統的軟體和硬件方面相關危害，其中包括IT-NETWORK、第三方來源軟體。	7.1 分析及識別軟體危害的情況
14.6.2 風險控制 藉由選擇及適當驗證的方式以實施每項風險控制措施，並確保每項風險控制措施都能降低已識別的風險。	5.1.4 軟體開發標準、方法及工具規劃 該標準要求確定一般用於開發的特定工具和方法，而不是每種風險控制措施。
14.7 規格要求 對於可程式化電子醫療系統及其每個子系統（例如，用於可程式化電子子系統），應有文件化的要求規範。 系統或子系統的要求規範應包括區分該系統或子系統實施的任何基本性能和任何風險控制措施。	5.2 軟體需求分析 該標準僅涉及可程式化電子醫療系統的軟體子系統。
14.8 架構 對於可程式化電子醫療系統及其每個子系統，應指定一個滿足要求規範的架構。	5.3 軟體架構設計
14.9 設計和實施 在適當的情況下，設計應分解為子系統，每個子系統都具有設計和測試規範。 有關設計環境的描述性數據應包含在文件檔案中。	5.4 軟體細部設計 5.4.2 開發每個軟體細部設計單元 該標準不要求軟體細部設計的測試規範。
14.10 驗證 所有實施基本安全、性能或風險控制措施的功能都需要驗證。	5.1.6 軟體驗證計劃 每項活動都需要驗證

（四）軟體組態管理

軟體組態管理應該記載主導的研究團隊成員個別於管理活動扮演的角色及工作範圍、軟體版本、軟體文件規劃及命名、變更控制、變更需求、更新需求及紀錄軟體生命週期之儲存、維護、變更和報告等過程，並追溯軟體系統所有活動。

（五）軟體風險管理

軟體風險管理通常以ISO 14971為基礎建構，從最小的軟體單元起至可程式化電子醫療系統(PEMS)皆應預估可能被預見的風險，並分析、評估該風險的嚴重程度，可以利用設計變更、測試數據或是警示標語等措施進行風險控制，後續再評估風險是否有降低至可接受範圍或產生新的風險可能，再利用驗證及確認評估總殘餘風險使否在可接受範圍內。由（表3）與ISO 14971:2007關係對照表軟體確效重視於預估軟體風險危害後實施風險措施經由驗證後是否在可接受範圍內。