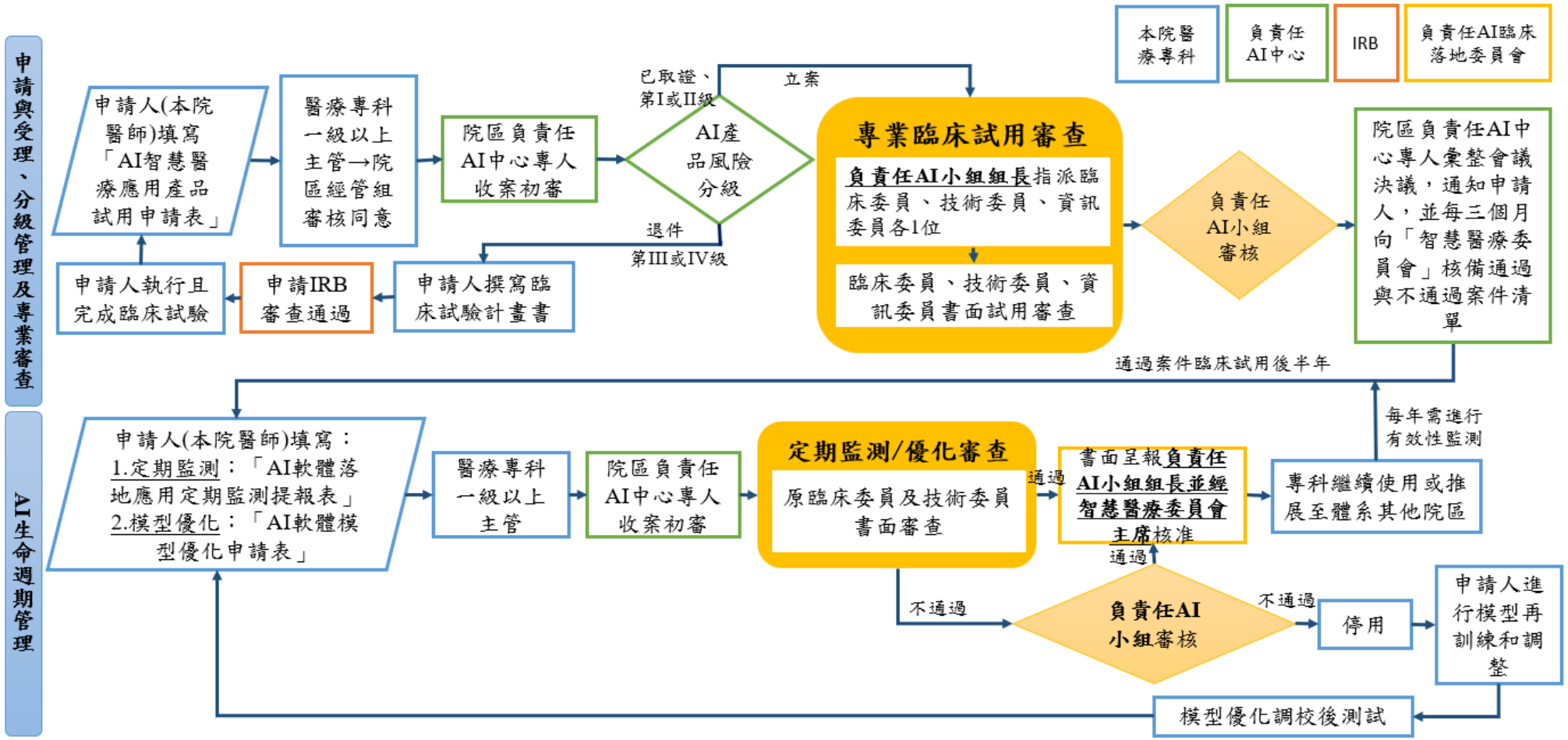
長庚醫療財團法人嘉義長庚紀念醫院
負責任 AI 臨床落地管理作業流程
目錄表

表一負責任 AI 臨床落地管理作業流程
附件一 AI 智慧醫療應用產品試用申請表
附件二 AI 智慧醫材軟體資安防護需求等級評估表
附件三 負責任 AI 執行申請產品及軟體資訊安全自評表
附件五 AI 軟體落地應用定期監測提報表
附件七 AI 軟體模型優化申請暨審查表

負責任 AI 臨床落地管理作業流程



AI 智慧醫療應用產品試用申請表

一、申請案基本資料

<table>
<tr><th colspan="2">AI 軟體基本資料</th></tr>
<tr><td>AI 軟體名稱</td><td>中文：
英文：</td></tr>
<tr><td>軟體敘述</td><td></td></tr>
<tr><td>軟體用途</td><td></td></tr>
<tr><td>適應症
(預期用途或效能)</td><td></td></tr>
<tr><td>預計適用科別</td><td></td></tr>
<tr><td>技術特點</td><td>☐電腦輔助篩檢 (Computer Aided Triage, CAT)
☐電腦輔助偵測 (Computer Aided Detection, CADe)
☐電腦輔助診斷 (Computer Aided Diagnosis, CADx)
☐其他_____</td></tr>
<tr><td>軟體效能</td><td>◆敏感度：
◆特異度：
◆陰性預測率：
◆陽性預測率：
◆準確度：
◆接收者操作特徵曲線下面積(AUC)：
(備註：此軟體效能指標將做為後續 AI 產品臨床試用後效能監測依據)</td></tr>
<tr><td>醫療器材軟體來源之產權查證</td><td>1.產權製造商名稱：
(備註：請上傳廠商該物件之產權文件或是已簽署之合約)。
2.本院是否有醫療器材智慧財產權(IP)歸屬：☐是☐否
3.智慧財產權歸屬說明：</td></tr>
<tr><td>通過許可證情形</td><td>☐已有台灣衛生福利部食品藥物管理署許可證(TFDA)，申請臨床試用。
☐已有美國食品藥品監督管理局(FDA)，但無 TFDA，申請臨床試用。
☐已有歐洲合格認證(CE) ，申請臨床試用。
☐無台灣或美國相關主管單位許可證，申請臨床試用。
☐其他，說明 請上傳 IRB 通過函及研究計畫書(protocal)</td></tr>
<tr><td>醫療器材軟體使用方式與目的簡要說明</td><td>(備註：可說明為改善診斷正確性、輔助醫療決策、取代大量 勞力工作、提升醫療風險預警時效)</td></tr>
<tr><td>AI 智慧醫材風險分級評估(依據美國 FDA)</td><td>1. 自評風險分級理由說明：
2.自評風險分級 (*必填)：☐第 I 級 ☐第 II 級 ☐第 III 級 ☐第 IV 級
<table>
<tr><td rowspan="2">醫療器材軟體適用之醫療照護情況</td><td colspan="3">提供的資訊對於醫療照護決策之重要性</td></tr>
<tr><td>治療或診斷</td><td>驅動(drive)臨床管理</td><td>告知(inform)臨床管理資訊</td></tr>
<tr><td>危急情況</td><td>IV</td><td>III</td><td>II</td></tr>
<tr><td>嚴重情況</td><td>III</td><td>II</td><td>I</td></tr>
<tr><td>非嚴重情況</td><td>II</td><td>I</td><td>I</td></tr>
</table></td></tr>
</table>

<table>
<tr><td>AI 產品九大透明性內容</td><td>請填寫此 AI 產品九大透明性內容
<table>
<tr><th colspan="2" rowspan="2">九大透明性內容</th><th colspan="2">AI 產品</th></tr>
<tr><th>AI1-1</th><th>AI1-2</th></tr>
<tr><td>介入詳情及輸出</td><td>Details and output of the intervention</td><td></td><td></td></tr>
<tr><td>介入目的</td><td>Purpose of the intervention</td><td></td><td></td></tr>
<tr><td>介入的警告範圍外使用</td><td>Cautioned Out-of-Scope Use of the intervention</td><td></td><td></td></tr>
<tr><td>介入開發詳情及輸入特徵</td><td>Intervention development details and input features</td><td></td><td></td></tr>
<tr><td>確保介入開發公平性的過程</td><td>Process used to ensure fairness in development of the intervention</td><td></td><td></td></tr>
<tr><td>外部驗證過程</td><td>External validation process</td><td></td><td></td></tr>
<tr><td>模型表現的量化指標</td><td>Quantitative measures of performance</td><td></td><td></td></tr>
<tr><td>介入實施和使用的持續維護</td><td>Ongoing maintenance of intervention implementation and use</td><td></td><td></td></tr>
<tr><td>更新和持續驗證或公平性評估計劃</td><td>Update and continued validation or fairness assessment schedule</td><td></td><td></td></tr>
</table></td></tr>
<tr><td colspan="2">AI 智慧醫療產品所屬系統資訊</td></tr>
<tr><td>主要運算硬體配置地點</td><td colspan="2">☐資訊室機房
☐臨床端設備，地點：</td></tr>
<tr><td>主要運算硬體設備廠牌/型號(*必填)</td><td colspan="2"></td></tr>
<tr><td rowspan="3">是否需要本院提供 GPU、CPU 等運算資源</td><td colspan="2">☐否
☐是，請續填以下 inference 時的使用資源之資訊：</td></tr>
<tr><td>儲存空間需求</td><td>_____GB
備註：請依 AI 軟體推展的院區數、模型數量與版次、軟體使用頻率、軟體使用人數，預估 AI 軟體「整體」使用的儲存空間，包含：模型軟體儲存空間、資料儲存空間、紀錄檔(log)儲存空間。</td></tr>
<tr><td>運算處理器需求</td><td>CPU：_____Cores
GPU：_____Cores
備註：申請上限 CPU 8 Cores、GPU 4 Cores，如有模型軟體需求超過此數量，需要特別評估。</td></tr>
</table>

<table>
<tr><td></td><td>記憶體需求</td><td>_____GB
備註：一個模型軟體(包括多院區使用與多版本使用)申請上限以 32 GB Memory 為原則。</td></tr>
<tr><td>AI 模型的提供方式</td><td colspan="2">☐模型檔，檔案類型如：h5、pth、onnx 等
☐Docker 封裝檔
☐詳列安裝環境套件版本
☐其他，請說明：</td></tr>
<tr><td>主要運算軟體配置-作業系統類型與版本</td><td colspan="2">☐Windows，版本：
☐Linux，版本：
☐其他，請說明</td></tr>
<tr><td>作業系統啟用之服務與連接埠</td><td colspan="2"><table><tr><td>範例：http</td><td>範例：80</td></tr><tr><td>範例：https</td><td>範例：443</td></tr><tr><td>http</td><td>80</td></tr><tr><td>tcp</td><td>8001</td></tr><tr><td>tcp</td><td>8002</td></tr></table>(備註：除必要之服務外，停用其他非必要之服務)</td></tr>
<tr><td>是否需安裝 client 軟體於院內電腦</td><td colspan="2">(備註:用戶端軟體安裝需求填寫範例如： 1. 可透過 IE/Chrome 瀏覽器直接使用(如另需安裝元件請務必說明） 2. 需安裝 uniweb client 軟體於影像醫學部/全院診間/病房)
☐是，請說明程式名稱版本及安裝地點：
☐否</td></tr>
<tr><td>網路連線型式</td><td colspan="2">☐有線
☐無線</td></tr>
<tr><td>網路連線速率要求</td><td colspan="2"></td></tr>
<tr><td>主機固定 IP 需求組數</td><td colspan="2"></td></tr>
<tr><td>是否對外連線</td><td colspan="2">☐是 ☐否</td></tr>
<tr><td>平均每筆檢查運算時間</td><td colspan="2"></td></tr>
<tr><td>推論結果回傳至系統</td><td colspan="2">☐獨立系統不回傳
☐HIS：☐門診醫囑系統、☐住診醫囑系統、☐急診醫囑系統、☐檢查報告系統、☐X光檢查報告系統、☐其他，請說明：
☐PACS
☐LIS
☐RIS
☐CIS(ICIP/ICCA)
☐Portal
☐院外系統，請說明：</td></tr>
<tr><td>回傳方式</td><td colspan="2">☐Web Service
☐API
☐資料庫中繼資料表
☐結果批次回傳，請說明(頻率/時段)
☐結果即時回傳</td></tr>
<tr><td>輸入資料大小、筆數預估(以每日最大量計算)</td><td colspan="2"><table><tr><td>欄位名稱</td><td>資料型別/大小</td><td>個資/去識別處理方式說明 (系統如與外連線，資料需去識別)</td></tr><tr><td></td><td></td><td>僅讀取像素資料，因此無個資資料</td></tr></table></td></tr>
<tr><td>需輸入的欄位說明，如有多項，請分點說明</td><td colspan="2"><table><tr><td>欄位名稱</td><td>資料型別/大小</td><td>個資/去識別處理方式說明</td></tr><tr><td></td><td></td><td></td></tr></table></td></tr>
</table>

輸入資料來源範圍篩選	(例如：特定區域、特定診斷/醫令/術式、特定儀器...) 備註：輸出的欄位說明，如有多項，請分點說明
輸出說明(試用輸出地點)	
試用者畫面呈現	
試用資訊內容	
試用者畫面樣式	否有 AI 智慧醫療器材軟體使用手冊(請檢附) ☐是 ☐否
系統架構圖	請說明並**檢附檔案：** (備註：包含與該服務主機連接的所有設備((client 端、儀器、switch...等))、架構網路拓樸(包含各設備開啟的 Port 與 Protocol)、資料串接 流程。以上可在同張圖上或是分多張說明皆可。
系統需介接醫院資訊 系統資料來源：	(此系統於院內分級將作為 AI 產品及所屬系統之資安防護等級依據，待回覆後續填覆第二部分資安評估)

申請人資料	
申請人	姓名： 電話： e-mail：
申請人所屬科別	
申請部門 一級主管	

二、醫療資訊安全評估(建議由開發單位資訊工程師填寫)

備註:

✧ 為維護資訊安全，系統上線後資訊室仍將持續進行資訊安全測試。如發現須改善之漏洞，管理單位(申請單位)應於收到通知後要求智慧醫材軟體供應者限期修正。如超過可接受風險，應停止試用至改善完成為止。

1. 本次試用之醫材軟體，過去是否已於本院通過試用申請程序 (*必填)
   ☐ 是
   ☐ 否

2. 是否已完成資安防護需求**等級評估(上傳檔案(1))**，資通系統防護需求等級：☐普☐中☐高

3. 是否已經依據等級回填**自評表(請參考資安法檢核表)(上傳檔案(2))**

4. 系統與程式安全性檢測(依據防護等級視需要提供)

檢 測 項 目	檢測產品	檢測產品之版本	檢測特徵版本	**上傳報告**
系統安全性檢測				系統安全性檢測範本(上傳檔案)(3)

程式動態檢測				程式動態檢測範本(上傳檔案)(4)
程式靜態(源碼)檢測				程式靜態(源碼)檢測範本(上傳檔案)(5)

備註：

- ✧ 安全性檢測皆需提供執行程式版本與特徵（檢測規則）版本
- ✧ 動態與靜態檢測均須列出檢測標的清單。
- ✧ 報告語言限制繁體中文或英文)

5. 系統與程式安全性檢測補充說明：

6. 資料傳輸採用之加密機制及版本：

7. 系統上線後故障處理機制---是否試用於緊急醫療處置情境

☐ 是

☐ 否→☐系統停止服務，回歸人工作業、 ☐其他，請說明

8. 旁路測試計畫(*必填)：旁路測試報告(檔案上傳)(6)
備註：旁路測試目的只是要確認在該 AI 服務中斷時，原本作業流程是否會受到影響，是否有 Bypass 該服務(設備)的方式。注意：這邊指的作業流程非僅限於和 Portal 相關作業，尚包含儀器 DICOM 上傳 PACS 或和本 AI 服務串接之設備相關日常作業，並請先行測試計畫可行性。

9. 備份還原計畫：

三、資料去識別、保存及銷毀管理機制(個資保護)

項目	自醫院端輸入資料	運算過程資料	運算結果資料
是否保留	☐保留 ☐不保留	☐保留 ☐不保留	☐保留 ☐不保留
是否去識別			☐是 ☐否
保留位置			☐回傳院內系統 ☐上傳院外系統 ☐其他，請說明
保留期限			
資料接觸人員權限管控機制			運算結果儲存於資料庫
試用結束後資料處理機制			☐交由資訊室處理 ☐交由計畫主持人處理 ☐刪除傳統磁碟與 SSD 內容 ☐其他，請說明
銷毀機制			

聲明：

1. 申請者、協同申請者以及單位主管皆保證此所提之醫療器材軟體內容敘述屬實。申請者願意負擔一切責任
2. 於嘉義長庚紀念醫院試用之醫療醫材軟體，不代表可作為商業使用之憑證

「智慧醫材軟體」資安防護需求等級評估表

主要功能說明：OOOO

評估日期：OO 年 OO 月 OO 日

影響構面				資安 防護需求等級
1.機密性	2.完整性	3.可用性	4.法律遵循性	

步驟❶：填寫醫材軟體基本資料

子功能軟體項目			
是否為「支持核心業務持續運作必要之核心資通系統」(Y/N)		是否含機敏資料(Y/N)	

步驟❷：設定影響構面等級

影響構面		防護需求等級	原因說明
1. 機密性	初估		
	異動		
2. 完整性	初估		
	異動		
3. 可用性	初估		
	異動		
4. 法律遵循性	初估		
	異動		

核章欄	
業務/系統承辦人	複核人員

附表名稱：負責任 AI 執行申請產品及軟體資訊安全自評表(含表一至表四)

表一、基本資料表(共通表單)

表二、資通系統防護基準檢核表(普級系統適用)

表三、資通系統防護基準檢核表(中級系統適用)

表四、資通系統防護基準檢核表(高級系統適用)

表一、基本資料表

資通系統名稱	
機關單位名稱	
填寫人員	
填寫日期	
審核人員	
附件項目條列	

表二、資通系統防護基準檢核表(普級系統適用)

構面	類別	項次編號(原始)	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
存取控制	帳號管理	1	普	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。						
	遠端存取	10	普	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。						
		11	普	使用者之權限檢查作業應於伺服器端完成。						
		12	普	應監控遠端存取機關內部網段或資通系統後臺之連線。						
		13	普	應採用加密機制。						
事件日誌與可歸責性	記錄事件	15	普	訂定日誌之記錄時間週期及留存政策，並保留日誌至少 6 個月。						
		16	普	確保資通系統有記錄特定事件之功能，並						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				決定應記錄之特定資通系統事件。						
		17	普	應記錄資通系統管理者帳號所執行之各項功能。						
	日誌紀錄內容	19	普	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。						
	日誌儲存容量	20	普	依據日誌儲存需求，配置所需之儲存容量。						
	日誌處理失效之回應	21	普	資通系統於日誌處理失效時，應採取適當之行動。						
	時戳及校時	23	普	資通系統應使用系統內部時鐘產生日誌所需時戳						

構面	類別	項次編號(原始)	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。						
	日誌資訊之保護	25	普	對日誌之存取管理，僅限於有權限之使用者。						
營運持續計畫	系統備份	28	普	訂定系統可容忍資料損失之時間要求。						
		29	普	執行系統源碼與資料備份。						
識別與鑑別	內部使用者之識別與鑑別	35	普	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。						
	身分驗證管理	37	普	使用預設密碼登入系統時，應於登入後要求立即變更。						
		38	普	身分驗證相關資訊不以明文傳輸。						
		39	普	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達5次後，至少15分鐘內不允許該						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				帳號繼續嘗試登入或使用機關自建之失敗驗證機制。						
		40	普	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。(對非內部使用者，可依機關自行規範辦理)						
		41	普	密碼變更時，至少不可以與前3次使用過之密碼相同。(對非內部使用者，可依機關自行規範辦理)						
		42	普	上述兩點所定措施，對非內部使用者，可依機關自行規範辦理。						
	鑑別資訊回饋	45	普	資通系統應遮蔽鑑別過程中之資訊。						
	非內部使用者之識別	47	普	資通系統應識別及鑑非機關使用者（或代表機關使用者行為之						

構面	類別	項次編號(原始)	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
	與鑑別			程序)。						
系統與服務獲得	系統發展生命週期需求階段	48	普	針對系統安全需求(含機密性、可用性、完整性)，進行確認。						
	系統發展生命週期開發階段	51	普	應針對安全需求實作必要控制措施。						
		52	普	應注意避免軟體常見漏洞及實作必要控制措施。						
		53	普	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。						
	系統發展生命週期測試階段	56	普	執行「弱點掃描」安全檢測。						
	系統發展生命週期部署與維運階段	58	普	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。						
		59	普	資通系統不使用預設						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				密碼。						
	系統發展生命週期委外階段	61	普	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。						
	系統文件	63	普	應儲存與管理系統發展生命週期之相關文件。						
系統與資訊完整性	漏洞修復	70	普	系統之漏洞修復應測試有效性及潛在影響，並定期更新。						
	資訊系統監控	72	普	發現資通系統有被入侵跡象時，應通報機關特定人員。						

表三、資通系統防護基準檢核表(中級系統適用)

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
存取控制	帳號管理	1	普	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。						
		2	中	已逾期之臨時或緊急帳號應刪除或禁用。						
		3	中	資通系統閒置帳號應禁用。						
		4	中	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。						
	最小權限	9	中	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。						
	遠端存取	10	普	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
		11	普	化。 使用者之權限檢查作業應於伺服器端完成。						
		12	普	應監控遠端存取機關內部網段或資通系統後臺之連線。						
		13	普	應採用加密機制。						
		14	中	遠端存取之來源應為機關已預先定義及管理之存取控制點。						
事件日誌與可歸責性	記錄事件	15	普	訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。						
		16	普	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。						
		17	普	應記錄資通系統管理者帳號所執行之各項功能。						
		18	中	應定期審查機關所保留資通系統產生之日誌。						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
	日誌紀錄內容	19	普	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。						
	日誌儲存容量	20	普	依據日誌儲存需求，配置所需之儲存容量。						
	日誌處理失效之回應	21	普	資通系統於日誌處理失效時，應採取適當之行動。						
	時戳及校時	23	普	資通系統應使用系統內部時鐘產生日誌所需時戳 ，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。						
		24	中	系統內部時鐘應定期與基準時間源進行同步。						
	日誌資訊之保	25	普	對日誌之存取管理，僅限於有權限之使用者。						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
	護	26	中	應運用雜湊或其他適當方式之完整性確保機制。						
營運持續計畫	系統備份	28	普	訂定系統可容忍資料損失之時間要求。						
		29	普	執行系統源碼與資料備份。						
		30	中	應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。						
	系統備援	33	中	訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。						
		34	中	原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。						
識別與鑑別	內部使用者之識別與鑑別	35	普	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。						
	身分驗證管理	37	普	使用預設密碼登入系統時，應於登入後要求立						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				即變更。						
		38	普	身分驗證相關資訊不以明文傳輸。						
		39	普	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達5次後，至少15分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。						
		40	普	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。(對非內部使用者，可依機關自行規範辦理)						
		41	普	密碼變更時，至少不可以與前3次使用過之密碼相同。(對非內部使用者，可依機關自行規範辦理)						
		42	普	上述兩點所定措施，對非內部使用者，可依機關自行規範辦理。						
		43	中	身分驗證機制應防範自						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				動化程式之登入或密碼更換嘗試。						
		44	中	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。						
	鑑別資訊回饋	45	普	資通系統應遮蔽鑑別過程中之資訊。						
	加密模組鑑別	46	中	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。						
	非內部使用者之識別與鑑別	47	普	資通系統應識別及鑑非機關使用者（或代表機關使用者行為之程序)。						
系統與服務獲得	系統發展生命週期需求階段	48	普	針對系統安全需求(含機密性、可用性、完整性)，進行確認。						
	系統發展生命週期設計階段	49	中	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
		50	中	將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正。						
	系統發展生命週期開發階段	51	普	應針對安全需求實作必要控制措施。						
		52	普	應注意避免軟體常見漏洞及實作必要控制措施。						
		53	普	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。						
	系統發展生命週期測試階段	56	普	執行「弱點掃描」安全檢測。						
	系統發展生命週期部署與維運階段	58	普	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。						
		59	普	資通系統不使用預設密碼。						
		60	中	於系統發展生命週期之維運階段，應執行版本						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				控制與變更管理。						
	系統發展生命週期委外階段	61	普	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。						
	獲得程序	62	中	開發、測試以及正式作業環境應為區隔。						
	系統文件	63	普	應儲存與管理系統發展生命週期之相關文件。						
系統與資訊完整性	漏洞修復	70	普	系統之漏洞修復應測試有效性及潛在影響，並定期更新。						
		71	中	定期確認資通系統相關漏洞修復之狀態。						
	資訊系統監控	72	普	發現資通系統有被入侵跡象時，應通報機關特定人員。						
		73	中	監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。						
	軟體及	75	中	使用完整性驗證工具，						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
	資訊完整性			以偵測未授權變更特定軟體及資訊。						
		76	中	使用者輸入資料合法性檢查應置放於應用系統伺服器端。						
		77	中	發現違反完整性時，資通系統應實施機關指定之安全保護措施。						

三、資通系統防護基準檢核表(高級系統適用)

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
存取控制	帳號管理	1	普	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。						
		2	中	已逾期之臨時或緊急帳號應刪除或禁用。						
		3	中	資通系統閒置帳號應禁用。						
		4	中	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。						
		5	高	機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。						
		6	高	逾越機關所許可之閒置時間或可使用期限						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				時，系統應自動將使用者登出。						
		7	高	應依機關規定之情況及條件，使用資通系統。						
		8	高	監控資通系統帳號，如發現帳號違常使用時回報管理者。						
	最小權限	9	中	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。						
	遠端存取	10	普	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件						
		11	普	化。 使用者之權限檢查作業應於伺服器端完成。						
		12	普	應監控遠端存取機關						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				內部網段或資通系統後臺之連線。						
		13	普	應採用加密機制。						
		14	中	遠端存取之來源應為機關已預先定義及管理之存取控制點。						
事件日誌與可歸責性	記錄事件	15	普	訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。						
		16	普	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。						
		17	普	應記錄資通系統管理者帳號所執行之各項功能。						
		18	中	應定期審查機關所保留資通系統產生之日誌。						
	日誌紀錄內容	19	普	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。						
	日誌儲存容量	20	普	依據日誌儲存需求，配置所需之儲存容量。						
	日誌處理失效之回應	21	普	資通系統於日誌處理失效時，應採取適當之行動。						
		22	高	機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。						
	時戳及校時	23	普	資通系統應使用系統內部時鐘產生日誌所需時戳 ，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
		24	中	系統內部時鐘應定期與基準時間源進行同步。						
	日誌資訊之保護	25	普	對日誌之存取管理，僅限於有權限之使用者。						
		26	中	應運用雜湊或其他適當方式之完整性確保機制。						
		27	高	定期備份日誌至原系統外之其他實體系統。						
營運持續計畫	系統備份	28	普	訂定系統可容忍資料損失之時間要求。						
		29	普	執行系統源碼與資料備份。						
		30	中	應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。						
		31	高	應將備份還原，作為營運持續計畫測試之一部分。						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
		32	高	應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。						
	系統備援	33	中	訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。						
		34	中	原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。						
識別與鑑別	內部使用者之識別與鑑別	35	普	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。						
		36	高	對資通系統之存取採取多重認證技術。						
	身分驗證管理	37	普	使用預設密碼登入系統時，應於登入後要求立即變更。						
		38	普	身分驗證相關資訊不以明文傳輸。						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
		39	普	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達5次後，至少15分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。						
		40	普	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。(對非內部使用者，可依機關自行規範辦理)						
		41	普	密碼變更時，至少不可以與前3次使用過之密碼相同。(對非內部使用者，可依機關自行規範辦理)						
		42	普	上述兩點所定措施，對非內部使用者，可依機關自行規範辦理。						
		43	中	身分驗證機制應防範						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				自動化程式之登入或密碼更換嘗試。						
		44	中	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。						
	鑑別資訊回饋	45	普	資通系統應遮蔽鑑別過程中之資訊。						
	加密模組鑑別	46	中	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。						
	非內部使用者之識別與鑑別	47	普	資通系統應識別及鑑非機關使用者（或代表機關使用者行為之程序 ）。						
系統與服務獲得	系統發展生命週期需求階段	48	普	針對系統安全需求(含機密性、可用性、完整性) ，進行確認。						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
	系統發展生命週期設計階段	49	中	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。						
		50	中	將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正。						
	系統發展生命週期開發階段	51	普	應針對安全需求實作必要控制措施。						
		52	普	應注意避免軟體常見漏洞及實作必要控制措施。						
		53	普	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。						
		54	高	執行「源碼掃描」安全檢測。						
		55	高	系統應具備發生嚴重錯誤時之通知機制。						
	系統發	56	普	執行「弱點掃描」安						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
	展生命週期測試階段			全檢測。						
		57	高	執行「滲透測試」安全檢測。						
	系統發展生命週期部署與維運階段	58	普	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。						
		59	普	資通系統不使用預設密碼。						
		60	中	於系統發展生命週期之維運階段，應執行版本控制與變更管理。						
	系統發展生命週期委外階段	61	普	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。						
	獲得程序	62	中	開發、測試以及正式作業環境應為區隔。						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
	系統文件	63	普	應儲存與管理系統發展生命週期之相關文件。						
系統與通訊保護	傳輸之機密性與完整性	64	高	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。						
		65	高	使用公開、國際機構驗證且未遭破解的演算法。						
		66	高	支援演算法的最大長度金鑰。						
		67	高	加密金鑰或憑證週期性更換。						
		68	高	伺服器端之金鑰保管應製定管理規則及實施應有之安全防護措施。						
	資料儲存之安全	69	高	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				以其他適當方式儲存。						
系統與資訊完整性	漏洞修復	70	普	系統之漏洞修復應測試有效性及潛在影響，並定期更新。						
		71	中	定期確認資通系統相關漏洞修復之狀態。						
	資訊系統監控	72	普	發現資通系統有被入侵跡象時，應通報機關特定人員。						
		73	中	監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。						
		74	高	資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。						
	軟體及資訊完整性	75	中	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。						
		76	中	使用者輸入資料合法						

構面	類別	項次編號（原始）	最低系統等級要求	安全控制措施	是否符合	現況說明	佐證	矯正作為	目標日期	備註說明
				性檢查應置放於應用系統伺服器端。						
		77	中	發現違反完整性時，資通系統應實施機關指定之安全保護措施。						
		78	高	應定期執行軟體和資訊完整性檢查。						

AI 軟體落地應用定期監測提報表

AI 軟體名稱	
軟體敘述	
AI 軟體試用申請人	院區： 單位/科別： 姓名：
目前使用院區	
目前使用科別	
臨床運用後 AI 軟體效能	◆敏感度： ◆特異度： ◆陰性預測率： ◆陽性預測率： ◆準確度： ◆接收者操作特徵曲線下面積(AUC)：
摘要說明目前臨床運用使用情形	1.「AI 軟體推論」是否列入臨床標準作業程序？ □是 □否 2.請說明目前使用病人數、使用醫師數： 3.效益：
AI 軟體推廣至其他院區或科別之規劃	□暫不推廣，請說明原因： □預計推展至其他院區/科別，請說明院區/科別： 推廣規劃說明：
送件聯絡人	姓名： 電話： e-mail：

AI 軟體模型優化申請暨審查表

AI 軟體基本資料	
AI 軟體名稱	
軟體敘述	
AI 軟體試用申請人	院區/單位/科別： 姓名：
演算法與開發工具	1.演算法名稱： 2.開發工具(如：python、R...)：
AI 模型修正/優化相關資料	
AI 軟體修正/優化原因	
AI 軟體修正/優化內容	
AI 軟體修正/優化後 效能驗證結果	1.修正後模型驗證資料的組成及樣本數： 2.軟體效能： ◆敏感度： ◆特異度： ◆陰性預測率： ◆陽性預測率： ◆準確度： ◆接收者操作特徵曲線下面積(AUC)：
修正/優化後 儲存空間需求	_____GB 備註：請依 AI 軟體推展的院區數、模型數量與版次、軟體使用頻率、軟體使用人數，預估 AI 軟體「整體」使用的儲存空間，包含：模型軟體儲存空間、資料儲存空間、紀錄檔(log)儲存空間。
修正/優化後 運算處理器需求	CPU：_____Cores GPU：_____Cores 備註：申請上限 CPU 8 Cores、GPU 4 Cores，如有模型軟體需求超過此數量，需要特別評估。
修正/優化後 記憶體需求	_____GB 備註：一個模型軟體(包括多院區使用與多版本使用)申請上限以 32 GB Memory 為原則。
修正/優化後 AI 模型的提供方式	☐模型檔，檔案類型如：h5、pth、onnx 等 ☐Docker 封裝檔 ☐其他，請說明：
送件聯絡人	姓名： 電話：　　e-mail：
以下由審查委員填寫	
審查意見	
審查結果	☐同意 AI 軟體之修正或優化 ☐建議說明後再書面審查 ☐建議提會複審 ☐不同意 AI 軟體之修正或優化
保密與利益迴避聲明暨委員簽名/日期	本人於本案審議過程中，確實遵守保密及利益迴避規範，並無發生利益衝突之情事，亦確實遵守保密責任。 委員簽名：_____　日期：_____