中華民國醫師公會全國聯合會
西醫基層醫療服務審查執行會暨分會
資訊安全事件通報與危機處理作業程序

106 年 1 月 1 日施行

壹、目的

為確保中華民國醫師公會全國聯合會西醫基層醫療服務審查執行會暨分會(以下簡稱「基層審查執行會暨分會」)於資訊安全事件發生時，得以迅速依程序進行通報，並採取必要之應變措施，特依據中華民國醫師公會全國聯合會西醫基層醫療服務審查執行會暨分會檔案資料管理辦法「柒、資訊安全事件通報與危機處理作業程序」規定，訂定本作業程序。

貳、權責

一、基層審查執行會暨分會：督導資訊安全事件之管理作業。

二、資訊安全小組：研擬資訊安全事件通報流程。

三、發現人員：基層審查執行會暨分會所有人員於發現(或疑似)資訊安全事件時，皆負有即時通報之責任。

四、權責單位：基層審查執行會暨分會。

五、資訊安全官：由基層審查執行會暨分會主任委員、副主任委員督導資訊安全事件通報、處理及分析作業。

六、緊急處理小組：

(一)確定事件影響範圍，並評估損失。

(二)協助資訊安全事件之通報、處理及分析作業。

參、名詞定義

一、資訊安全事件：凡於作業環境中，導致資訊資產之機密性、完整性、可用性遭受影響之事件。

二、內部危安事件：發現(或疑似)遭人為惡意破壞毀損、作業不慎等事件。

三、外力入侵事件：發現(或疑似)電腦病毒感染事件、駭客攻擊(或非法入侵)等事件。

四、天然災害：颱風、水災、地震等。

五、突發事件：其他導致資訊網路系統中斷事件等。

肆、作業說明

一、資訊安全事件之管理

(一)基層審查執行會暨分會應建立資訊安全事件之處理作業程序，並賦予相關人員必要責任，以便迅速有效處理資訊安全事件。

(二)除正常應變計畫(如：系統及服務之回復作業)，資訊安全事件之處理程序，應視需要納入下列事項：

1.導致資訊安全事件原因之分析。

2.防止類似事件再發生之補救措施。

3.電腦稽核軌跡及相關證據之蒐集。

4.與受影響之使用者進行溝通及說明。

(三)電腦稽核軌跡及相關證據應以適當方法保護，以利下列管理作業：

1.作為研析問題之依據。

2.作為研析是否違反契約或資訊安全規定之證據。

3.作為求償之依據。

(四)應依據「資訊安全事件通報與應變作業流程」處理資訊安全事件。相關作業程序應注意下列事項：

1.考量單位資源，於最短的時間內，確認回復後之系統及相關安全控制是否完整及正確。

2.向主任委員報告處理情形，並檢討、分析資訊安全事件。

3.限定僅授權之人員可使用回復後正常作業之系統及資料。

4.緊急處理步驟應詳實記載，以備日後查考。

二、通報程序

(一)疑似資訊安全事件發生時，發現人員應依事件歸屬通報權責單位。

(二)權責單位於收到通知後，應研判是否為資訊安全事件。若：

1.判定為非資訊安全事件時，應將結果回覆予發現人員。

2.判定為資訊安全事件時，應初估事件處理時間，並通知資訊安全官。

3.資訊安全事件等級區分為：

A 級：符合下列任一情形者：

(1)機密資料遭洩漏。

(2)關鍵業務系統或資料遭嚴重竄改。

(3)關鍵業務系統運作停頓，無法於可容忍中斷時間內回復正常運作。

B 級：符合下列任一情形者：

(1)敏感資料遭洩漏。

(2)關鍵業務系統或資料遭竄改。

(3)關鍵業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

C 級：符合下列任一情形者：

(1)限閱等級資料之關鍵業務系統或資料遭洩漏。

(2)關鍵業務系統或資料遭輕微竄改。

(3)關鍵業務運作遭影響或系統效率降低，於可容忍中斷時間內回

復正常運作。

D 級：符合下列任一情形者：

(1)非關鍵業務系統或資料遭洩漏。

(2)非關鍵業務系統或資料遭竄改。

(3)非關鍵業務運作遭影響或短暫停頓可立即修復。

(三)權責單位於發生資訊安全事件時，應立即填具「中華民國醫師公會全國聯合會西醫基層醫療服務審查執行會暨分會資訊安全事件報告單」(附件)。

(四)決策處理：

1.當事件影響較低、衝擊性較小，或僅涉及單位內部、受損程度輕微時(如：電腦病毒感染)，由權責單位自行處理，並將處理後狀況通知資訊安全官。

2.處理過程中如發現造成之影響大於原先判定事件，權責單位應立即向資訊安全官報告，重新執行事件分析辨識。

三、危機處理程序

基層審查執行會暨分會資訊安全危機處理包括事前建置安全防護機制、事中主動預警與緊急應變，以及事後復原追蹤鑑識偵查等步驟。說明如下：

(一)事前建置安全防護機制：

1.建置資訊安全管理系統及整體防護架構。

2.彙整及備妥資訊安全相關文件。

(二)事中主動預警與緊急應變：

1.事件辨識：辨識事件之歸屬及採取之對策，如內部資安事件、外力入侵事件、天然災害或重大突發事件等，並決定處理方法與程序。

2.事件控制：依據各類事件危機處理之程序，進行事件傷害控制，降低影響程度及範圍。

3.問題解決：事件處理權責單位須將問題解決。

4.恢復作業：問題解決後，系統需恢復至事件發生前之正常運作狀態。

(三)事後復原追蹤鑑識偵查：

1.後續追蹤之精神乃係檢討相關資訊安全事件是否會重複發生，並審視現有環境漏洞，透過研析相關資料，以釐清事件發生之原因與責任。

2.受損單位依復原程序實施災後復原重建。

附件

中華民國醫師公會全國聯合會西醫基層醫療服務審查執行會暨分會
資訊安全事件報告單

紀錄編號：_____　　填表日期：　　年　　月　　日

通報單位聯絡資料			
權責單位		發現人員	
電　　話		電子郵件	

資訊安全事件通報事項	
發生時間	____年____月____日____時____分至____年____月____日____時____分
設備資料	IP 位址(無；可免填)： Web 位址(無；可免填)： 設備廠牌、機型(請併填購買日期、使用期限)： 作業系統名稱、版本(請併填購買日期、使用期限)： 已裝置之安全機制：

資訊安全事件資料				
事件影響等級	□A 級	□B 級	□C 級	□D 級
事件分類	□非法入侵	□感染病毒	□阻斷服務	□其他
破壞程度	□系統當機	□資料庫毀損	□網頁遭篡改	□其他
事件說明				
可能影響範圍及損失評估				
應變措施				

期望支援項目

解決辦法	
解決時間	____年____月____日____時____分

權　責　單　位　承　辦　人	資　訊　安　全　官

※事件影響等級說明

資訊安全事件依影響等級區分為 4 個級別，由重至輕分別為「A 級」、「B 級」、「C 級」及「D 級」。

1.A 級事件，符合下列任一情形者：

(1)機密資料遭洩漏。

(2)關鍵業務系統或資料遭嚴重竄改。

(3)關鍵業務系統運作停頓，無法於可容忍中斷時間內回復正常運作。

2.B 級事件，符合下列任一情形者：

(1)敏感資料遭洩漏。

(2)關鍵業務系統或資料遭竄改。

(3)關鍵業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

3.C 級事件，符合下列任一情形者：

(1)限閱等級資料之關鍵業務系統或資料遭洩漏。

(2)關鍵業務系統或資料遭輕微竄改。

(3)關鍵業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

4.D 級事件，符合下列任一情形者：

(1)非關鍵業務系統或資料遭洩漏。

(2)非關鍵業務系統或資料遭竄改。

(3)非關鍵業務運作遭影響或短暫停頓可立即修復。