法規名稱：醫院個人資料檔案安全維護計畫實施辦法

修正日期：民國 111 年 09 月 23 日

第 1 條

本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。

第 2 條

本辦法適用範圍，為醫院蒐集、處理及利用之病歷或醫療個人資料。

第 3 條

本辦法所稱主管機關：在中央為衛生福利部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第 4 條

1 本辦法用詞，定義如下：

一、醫院：指總床數達一百床以上之私立醫院、醫療法人醫院及其他法人附設醫院。

二、所屬人員：指醫院執行業務之過程，接觸個人資料之人員。

三、專責人員：指醫院指定，負責規劃、訂定、修正及執行個人資料檔案安全維護計畫（以下簡稱安全維護計畫），及業務終止後個人資料處理方法與其他相關事項，並應定期向醫院提出報告之人員。

四、查核人員：指醫院指定，負責評核安全維護計畫執行情形及成效之人員。

2 前項第三款與第四款人員，不得為同一人。

第 5 條

1 醫院應依本辦法規定訂定安全維護計畫，其應載明事項如下：

一、個人資料蒐集、處理及利用之內部管理程序。

二、個人資料之範圍及項目。

三、人員管理及教育訓練。

四、設備安全管理。

五、個人資料安全事故之預防、通報及應變機制。

六、使用紀錄、軌跡資料及證據保存。

七、業務終止後，個人資料處理方法。

八、個人資料安全維護之整體持續改善方案。

九、資料安全管理及稽核機制。

2 前項安全維護計畫，應報直轄市、縣（市）主管機關備查；修正時，亦同。

第 6 條

前條安全維護計畫，應依醫院業務規模及特性，衡酌經營資源之合理分配，規劃、訂定、檢討或修正安全維護措施，落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第 7 條

1 醫院訂定第五條第一項第一款個人資料蒐集、處理及利用之內部管理程序及第二款個人資料之範圍及項目時，應確認蒐集個人資料之特定目的及其必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。

2 醫院經定期檢視，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期間屆滿而無保存必要者，應依第五條第一項第八款及醫療法第七十條規定，刪除、銷毀、停止蒐集、處理、利用或為其他適當之處置。

第 8 條

1 醫院於蒐集個人資料時，應符合前條第一項所定之類別及範圍。

2 醫院於傳輸個人資料時，應採取必要保護措施；國際傳輸電子病歷時，並應符合醫療機構電子病歷製作及管理辦法之規定。

第 9 條

1 醫院於蒐集個人資料時，應遵守本法第八條及第九條有關告知義務之規定，並依直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。

2 前項告知，其他法規另有規定者，從其規定。

第 10 條

醫院委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託人依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。

第 11 條

醫院應依第五條第一項第一款規定，對其所屬人員採取下列措施：

一、依據業務作業需要，建立管理機制，設定所屬人員權限，控管其接觸個人資料，並定期確認權限內容之必要性及適當性。

二、檢視各相關業務之性質，規範個人資料蒐集、處理、利用及其他相關流程之負責人員。

三、要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。

四、取消所屬人員離職時之存取權限，並要求將執行業務所持有之文件、資料，辦理交接，不得攜離使用。

第 12 條

醫院應依第五條第一項第三款規定，使所屬人員明瞭個人資料保護相關法令規定、責任範圍、作業程序及應遵守之相關措施。

第 13 條

1 醫院應依第五條第一項第四款規定，對所持有之個人資料檔案，設置必要之安全設備及防護措施。

2 前項安全設備及防護措施，應包括下列事項：

一、訂定各類設備或儲存媒體之使用規範。

二、個人資料內容於蒐集、處理或利用時，訂定並採取適當之加密措施或配置安全防護系統。

三、個人資料有備份之需要時，訂定備份機制、管理及保護程序。

四、訂定資料之銷毀程序，包括電腦、自動化機器或其他儲存媒介物於報廢、汰換或轉作其他用途時，確保個人資料完全移除或清除，無洩漏之虞。

第 13-1 條

1 前條個人資料檔案使用資通訊系統蒐集、處理或利用時，應訂定並採取下列資訊安全措施：

一、使用者身分確認及保護措施。

二、個人資料顯示之隱碼措施及使用時機。

三、網際網路傳輸之安全加密措施。

四、個人資料檔案及資料庫之存取控制與保護監控措施。

五、防止外部網路入侵措施。

六、非法或異常使用行為之監控及因應措施。

2 前項第五款及第六款措施，應定期演練及檢討改善。

第 14 條

1 醫院應依第五條第一項第五款規定，於發生個人資料被竊取、洩漏、竄改、毀損、滅失或其他侵害事故時迅速處理，以保護當事人之權益。

2 前項處理應包括下列事項：

一、採取適當之措施，控制事故對當事人造成之損害。

二、查明事故發生原因及損害狀況，以適當方式通知當事人或其法定代理人，並於發現事故時起七十二小時內，以書面通報直轄市、縣（市）主管機關及副知中央主管機關。

三、研議並採取避免事故再度發生之改進措施。

3 直轄市、縣（市）主管機關就所轄醫院個人資料發生第一項事故之完整處理情形，應按季通報中央主管機關。

4 直轄市、縣（市）主管機關接受第二項通報後，得依本法第二十二條至第二十五條規定，對該醫院為適當之監督管理措施；中央主管機關認有必要時，得督導直轄市、縣（市）主管機關對於該

醫院之相關監督管理機制。

5 第二項第二款通報紀錄格式及第三項按季通報紀錄格式，規定如附件一及附件二。

第 15 條

1 醫院應依第五條第一項第六款規定，採行適當措施，留存個人資料使用紀錄、自動化機器設備之軌跡資料或其他相關之證據資料，並於必要時提供說明。

2 前項紀錄與資料，應至少留存六個月。但法令另有規定者，不在此限。

第 16 條

1 醫院應依第五條第一項第七款規定，對業務終止後，其保有個人資料，依下列方式為之，並製作紀錄：

一、銷毀：銷毀之方法、時間、地點及證明。

二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

2 前項紀錄，應至少留存五年。但法令另有規定者，不在此限。

第 17 條

醫院應依第五條第一項第八款規定，參酌安全維護計畫執行狀況、技術發展、法令依據修正及其他因素，檢視所定安全維護計畫之合宜性，必要時應予修正。

第 18 條

1 查核人員應每年評核安全維護計畫之執行情形及成效，並將評核結果，向醫院提出報告。

2 醫院應依據前項評核結果，責成專責人員檢討、修正安全維護計畫之執行事項。

3 直轄市、縣（市）主管機關應定期查核第一項評核結果。

第 19 條

本辦法於公立醫院，準用之。

第 20 條

1 本辦法自發布後六個月施行。

2 本辦法修正條文自發布日施行。