醫院個人資料檔案安全維護計畫實施辦法

第一條　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。

第二條　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。

第三條　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。

第四條　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。

前項第三款與第四款人員，不得為同一人。

第五條　　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。

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。

第六條　　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。

第七條　　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。

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。

第八條　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。

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。

第九條　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。

前項告知，其他法規另有規定者，從其規定。

第十條　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。

第十一條　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。

第十二條　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。

第十三條　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。

前項安全設備及防護措施，應包括下列事項：

一、紙本資料檔案之安全保護設施及管理程序。

二、電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。

三、電子資料檔案之備份機制及管理程序。

四、紙本資料之銷毀程序；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，應採取適當措施，確保個人資料完全移除，避免洩漏。

第十四條　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、竄改或其他侵害事故時迅速處理，以保護當事人之權益。

醫院執行前項應變機制，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，並通報主管機關。

三、研議改進措施，避免事故再度發生。

前項第二款通報作業流程及文件書表格式，由直轄市、縣(市)主管機關公告之。

第十五條　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。

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。

第十六條　　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。

前項紀錄，應至少留存五年。但法令另有規定者，不在此限。

第十七條　　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。

第十八條　　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。

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。

直轄市、縣(市)主管機關應定期查核第一項評核結果。

第十九條　　本辦法於公立醫院，準用之。

第二十條　　本辦法自發布後六個月施行。