醫院個人資料檔案安全維護計畫實施辦法總說明

個人資料保護法(以下簡稱本法)第二十七條規定：「(第一項)非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。(第二項)中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。(第三項)前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」。

為加強醫院對於個人資料之保護措施，維護個人資料之安全性與正確性，並建立對個人資料之管理、稽核、保存及改善機制，爰依上開規定之授權，訂定「醫院個人資料檔案安全維護計畫實施辦法」(以下簡稱本辦法)，重點如下：

一、法源依據。(第一條)

二、本辦法之適用範圍。(第二條)

三、本辦法之主管機關。(第三條)

四、本辦法之用詞定義。(第四條)

五、醫院應訂定安全維護計畫。(第五條)

六、醫院應落實個人資料檔案之安全維護計畫。(第六條)

七、醫院所保有之個人資料，經定期檢視，應予刪除、銷毀或停止蒐集、處理及利用之情形。(第七條)

八、醫院蒐集及傳輸個人資料時應符合之規定。(第八條)

九、醫院蒐集個人資料應遵守之告知義務。(第九條)

十、醫院委託他人蒐集、處理或利用個人資料之規範。(第十條)

十一、醫院應對其所屬人員採取之措施。(第十一條)

十二、醫院應定期對所屬人員施以教育訓練或認知宣導，以落實本辦法之執行。(第十二條)

十三、醫院應設置必要之安全設備及防護措施。(第十三條)

十四、醫院應訂定應變機制。(第十四條)

十五、醫院應留存個人資料使用紀錄、自動化機器設備之軌跡資料。(第十五條)

十六、醫院於業務終止後，對其保有之個人資料之處理方法及留存紀錄。（第十六條）

十七、醫院應檢視所定計畫之合宜性，以持續改進個人資料保護機制。（第十七條）

十八、醫院應訂定個人資料檔案安全維護查核機制。（第十八條）

十九、公立醫院準用本辦法。（第十九條）

二十、本辦法施行日。（第二十條）

醫院個人資料檔案安全維護計畫實施辦法

條文	說明
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。	個人資料保護法第二十七條規定：「(第一項)非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。(第二項)中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。(第三項) 前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」，爰明定本辦法之法源依據。
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。	一、明定本辦法之適用範圍。 二、本辦法適用範圍以外之個人資料檔案，仍應依本法第二十七條第一項規定辦理。
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。	明定本辦法之主管機關。
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。	一、依據本法第二十七條第二項規定，指定總床數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，應訂定個人資料檔案安全維護計畫。總床數係指醫療機構設置標準第十五條一般病床及特殊病床數之總和。 二、為使安全維護計畫有效運作，爰責成醫院應指定專責人員及查核人員，並賦予其職務。 三、為確保查核制度獨立及確實執行，爰於第二項明定專責人員與查核人員不得為同一人。
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。	參考本法施行細則第十二條第二項規定，明定醫院依本辦法規定訂定安全維護計畫應包括之項目，且該計畫之訂定及修正應報地方主管機關備查。

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。	適用本辦法之醫院應配置相當資源，俾規劃、訂定、檢討、修正與執行安全維護計畫之相關事項，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。	一、醫院應依本法施行細則第十二條第二項第二款之規定，於安全維護計畫中就界定個人資料範圍相關事項加以規定，爰於第一項明定之。 二、為維護當事人權益，爰於第二項明定醫院對個人資料應定期檢視及清查，並為適當處置。
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。	一、第一項明定醫院蒐集個人資料，應符合前條第一項所定之類別及範圍。 二、配合本法施行細則第十二條第二項第五款規定有關蒐集、處理及利用之內部管理程序事項，爰於第二項明定醫院如有傳輸個人資料之情事，應採取必要保護措施；國際傳輸電子病歷時，應遵循醫療機構電子病歷製作及管理辦法之規定，以利個人資料安全維護。 三、必要保護措施，指避免個人資料被竊取、竄改、毀損、滅失或洩漏所採取之作為。
第九條　醫院於蒐集個人資料時，應遵	一、明定醫院應依本法第八條及第九條

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。	規定，採取適當告知方式以履行告知義務。 二、直接蒐集個人資料，係指向當事人蒐集個人資料；間接蒐集個人資料，係指蒐集非由當事人提供之個人資料。 三、第二項所定其他法規，如醫療法第六十三條、第六十四條、第七十九條、病人自主權利法第六條、安寧緩和醫療條例第七條。
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。	明定醫院委託他人蒐集、處理或利用個人資料之全部或一部時之規範。
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。	醫院及其所屬人員，不論是何種法律關係，醫院都應避免其保管、蒐集、處理及利用個人資料時，違反個人資料保護相關法令規定，導致侵害當事人權益情事，爰明定應採取必要且適當之管理措施。
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。	醫院應對所屬人員施以教育訓練或認知宣導，以落實本辦法之執行。
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	一、為確保醫院所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，爰於第一項明定，醫院對所保有之個人資料，應設置必要之安全設備及採取必要之防護措施。 二、第二項明定安全設備或防護措施之內涵。 三、本條所定防護措施，得參考本法施行細則第十二條規定辦理，相關實

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。	例如各類儲存媒體之保護、媒體傳輸等規範。
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。	一、本法第十二條規定，非公務機關所持有之個人資料發生被竊取、洩漏、竄改或其他侵害事故者，應查明後以適當方式通知當事人或其法定代理人，爰於第一項明定醫院在安全維護計畫中應訂定通報及應變機制。 二、第二項明定應變機制應包括事項，俾利發生個人資料外洩時，得迅速遵循處理，以保護當事人權益，並應通報其主管機關。
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。	醫院為證明確實執行安全維護計畫，已盡防止個人資料遭侵害之義務，應視其規模及業務性質採行適當措施，留存相關證據至少六個月，以供日後發生問題時提供說明佐證，以釐清其法律責任。
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。	一、醫院於業務終止後，應作妥善處置，不得再繼續使用其所保有之個人資料檔案。醫院應視其終止業務之原因，將所保有之個人資料予以銷毀、移轉或其他方式處理。 二、第一項明定醫院將所保有之個人資料予以銷毀、移轉或其他方式處理過程中，應記錄其方法、時間、地點、接受移轉資料之對象及合法移轉依據等資料，以便日後得以提出舉證。 三、依本法第三十條規定：「損害賠償請求權，自請求權人知有損害及賠償

	義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。」爰於第二項明定銷毀、移轉、刪除、停止處理或利用個人資料之紀錄至少應留存五年。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。	明定醫院應參酌相關因素，依據實務運作及法令變化等情形，檢視或修正安全維護計畫。
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。	一、為確保個人資料維護安全措施發生效能，明定醫院應訂定個人資料檔案安全維護評核機制，定期或不定期檢查安全維護計畫之執行情形。依本法第五十條規定，對非公務機關之代表人，因該非公務機關依本法第四十七條至第四十九條規定受罰鍰處罰時，除能證明已盡防止義務者外，應受同一額度罰鍰，爰規定向醫院提出評核結果報告，促使醫院得據以監督安全維護計畫之執行事項，落實對個人資料保護之工作。 二、明定地方主管機關應定期查核評核結果。
第十九條　本辦法於公立醫院，準用之。	本法第二條第七款定義，公務機關指依法行使公權力之中央或地方機關或行政法人；另依法務部一百零四年一月三十日法律字第一〇四〇三五〇〇四九〇號函略以，公立醫院亦行使部分之公權力行為，故屬本法上之「公務機關」。惟現行法令對於公務機關實施個人資料檔案安全維護，尚未有明確規範，且公立醫院對於個人資料檔案保護之義務與其他醫院相當，為使公立醫院落實個人資料安全維護措施，爰使公立醫院準用本辦法。
第二十條　本辦法自發布後六個月施行。	考量醫院保有之個人資料檔案數量龐大且複雜度高，爰明定本辦法自發布後六個月施行。