護理機構個人資料檔案安全維護計畫辦法草案總說明

依個人資料保護法第二十七條規定，非公務機關應採行適當之安全措施，防止所保有之個人資料被竊取、竄改、毀損、滅失或洩漏，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，並訂定相關計畫及處理方法之標準等相關事項之辦法。

為加強護理機構對於個人資料之保護措施，爰依個人資料保護法第二十七條第三項授權，訂定「護理機構個人資料檔案安全維護計畫辦法」(以下簡稱本辦法)草案，共計二十二條，內容重點如下：

一、 本辦法之法源依據及適用對象。(草案第一條、第二條)

二、 指定專人或建立專責組織負責個人資料保護及管理、清查所保有個人資料之種類與數量、個人資料之風險評估及管理機制、事故之預防、通報及應變機制。(草案第三條至第六條)

三、 個人資料之界定及管理措施、應行告知義務、委託他人蒐集、處理或利用個人資料之監督、利用個人資料行銷之方式、個人資料為國際傳輸前應遵循事項、當事人行使權利之方式、確保個人資料正確性之措施。(草案第七條至十四條)

四、 有關資料安全管理、人員管理、環境管理等事項。(草案第十五條至第十七條)

五、 有關安全維護計畫之稽核、記錄保存及改善等事項。(草案第十八條至第二十一條)

六、 本辦法之施行日期。(草案第二十二條)

護理機構個人資料檔案安全維護計畫辦法(草案)

條文	說明
第一章　總則	章名
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。	本辦法之法源依據。
第二條　本辦法所稱護理機構,指一般護理之家、產後護理機構及居家護理機構。但不包含公立護理機構。 護理機構應訂定個人資料檔案安全維護計畫（以下簡稱本計畫),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。 前項計畫,應包括業務終止後個人資料處理方法等相關個人資料管理事項。	一、依據本法第二十七條第二項規定，指定護理機構應依本辦法規定之相關組織及程式要求，訂定個人資料檔案安全維護計畫。 二、公立護理機構係屬個人資料保護法之公務機關，不適用本辦法之規定。
第二章　個人資料保護規劃	章名
第三條　護理機構應依其業務規模及特性，指定專人或建立專責組織，並考量資源之合理分配，配置相當資源。 前項專人或專責組織之任務如下： 一、規劃、訂定、修正與執行本計畫等相關事項，並定期向護理機構負責人報告。 二、訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。 三、定期對所屬人員施以個人資料保護認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之	配合本法施行細則第十二條第二項第一款、第七款規定,明定護理機構應配置相當人力、資源,以執行相關任務；另為利護理機構負責人善盡督導之責,明定個人資料檔案安全維護專人或專責組織應定期向負責人報告相關執行情況。

條文	說明
責任範圍及各種個人資料保護事項之方法或管理措施。	
第四條　護理機構應確認蒐集個人資料之特定目的，依特定目的之必要性，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。 護理機構經定期檢視，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、期限屆滿而無本法第十一條第三項但書者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置。	配合本法施行細則第十二條第二項第二款規定有關界定個人資料範圍事項，明定護理機構應定期查核及界定個人資料之範圍，以利個人資料安全維護。
第五條　護理機構應依前條界定之個人資料範圍及其業務涉及個人資料蒐集、處理、利用之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當管理機制。	配合本法施行細則第十二條第二項第三款規定有關個人資料風險評估及管理機制事項，明定護理機構應分析判斷於蒐集、處理及利用過程中，個人資料安全可能發生之風險，俾採行適當管控措施保護個人資料，以降低風險。
第六條　護理機構為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱事故），應訂定下列應變、通報及預防機制： 一、應變處理機制： （一）控制當事人損害之方式。 （二）查明事故後通知當事人之適當方式。 （三）應通知當事人事故事實、損害狀況、所為因應措施及諮詢服務專線等內容。 二、事故通報機制：事故發生後應受通報之內外部對象及其通報方式。 三、檢討預防機制：研議矯正預防措施，避免類似事故再次發生。 護理機構遇有重大個人資料事故者，應通報直轄市、縣(市)政府。	配合本法施行細則第十二條第二項第四款規定有關事故之預防、通報及應變機制事項，明定護理機構應採取之因應措施，以降低或控制損害，並讓當事人了解相關狀況，使當事人亦能採取相關措施防止損害發生或擴大，此外，亦應研議預防機制，防杜事故發生。

條文	說明
前項所稱重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及護理機構正常營運或大量當事人權益之情形。	
第三章　個人資料之管理程序及措施	章名
第七條　護理機構於蒐集、處理或利用個人資料包含本法第六條第一項規定之特種個人資料前，應於本計畫中建立下列作業程序： 一、 確認蒐集、處理個人資料具有特定目的及法定情形；其經當事人書面同意者，並應符合本法第七條第一項規定。 二、 確認利用個人資料於蒐集之特定目的必要範圍內；於特定目的外利用個人資料時，應檢視是否具備法定特定目的外之利用要件；其經當事人書面同意者，並應符合本法第七條第二項規定。 三、 確認一般個人資料及本法第六條第一項規定之特種個人資料之屬性，分別訂定管理程序。	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，明定護理機構應依個人資料之屬性訂定管理程序，並應遵循本法有關蒐集、處理及利用人資料之特定目的及法定要件，以利個人資料安全維護。
第八條　護理機構為遵守本法第八條及第九條有關蒐集個人資料之告知義務規定，應就下列事項建立相關程序： 一、 檢視蒐集、處理個人資料之特定目的。 二、 檢視蒐集、處理之個人資料，是否符合免告知之事由；其不符者，依據資料蒐集之情形，採取適當之告知方式。	依本法第八條及第九條非公務機關原則上應適時履行告知義務之規定，並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，明定護理機構應遵循本法有關告知義務之方式，以利個人資料安全維護。
第九條　護理機構利用個人資料為行銷時，應明確告知當事人其護理機構名稱及個人資料之取得來源。	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，明定護理機構應遵循本

條文	說明
護理機構於首次利用個人資料為行銷時，應提供當事人免費表示拒絕接受行銷之方式，並支付所需費用；當事人表示拒絕行銷後，應立即停止利用其個人資料行銷，並週知所屬人員。	法有關行銷規範，以利個人資料安全維護。
第十條　護理機構委託他人蒐集、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，明確約定相關監督事項與方式。	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，明定護理機構應遵循本法施行細則有關委託他人蒐集、處理或利用個人資料所應負之監督責任，以利個人資料安全維護。
第十一條　護理機構為維護其所保有個人資料之正確性，應採取下列方式為之： 一、 檢視個人資料於蒐集、處理或利用過程，是否正確。 二、 當發現個人資料不正確時，適時更正或補充。 三、 個人資料正確性有爭議者，應依本法第十一條第二項規定處理。 因可歸責於護理機構之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。	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，明定護理機構應遵循本法有關資料正確性之規範，以利個人資料安全維護。
第十二條　護理機構為提供資料當事人行使本法第三條所規定之權利，應採取下列方式為之： 一、 確認是否為個人資料之本人，或經其委託授權。 二、 提供當事人行使權利之方式，並遵守本法第十三條有關處理期限之規定。 三、 告知是否酌收必要成本費用。 四、 有本法第十條但書、第十一條第二項但書或第三項但書得	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，明定護理機構應遵循本法有關資料當事人行使權利之規範，以利個人資料安全維護。

條文	說明
拒絕當事人行使權利之事由，應附理由通知當事人。	
第十三條　護理機構應定期確認其所保有個人資料之特定目的是否消失及期限是否屆滿，如特定目的消失或期限屆滿時，應依本法第十一條第三項規定刪除、停止處理或利用。	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，明定護理機構應遵循本法有關特定目的消失與期限屆滿之處理規範，以利個人資料安全維護。
第十四條　護理機構進行個人資料國際傳輸前，應檢視有無衛生福利部依本法第二十一條規定為限制國際傳輸之命令或處分，並應遵循之。	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，明定護理機構應遵循本法有關國際傳輸規範，以利個人資料安全維護。
第十五條　護理機構為維護所保有個人資料之安全，應採取下列資料安全管理措施： 一、運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，訂定使用可攜式設備或儲存媒體之規範。 二、針對所保有之個人資料內容，有加密之需要者，採取適當之加密機制。 三、作業過程有備份個人資料之需要時，應比照原件，依本法規定予以適當保護。儲存備份資料之媒介物，以適當方式保管，且定期進行備份資料之還原測試，以確保有效性。 四、傳輸個人資料時，因應不同之傳輸方式，應採取必要保護措施；確認是否有加密之必要，如有必要，應採取適當之加密機制，並確認資料收受者之正確性。 五、妥善保存認證機制及加密機制中所運用之密碼，如有交付他人之需要，亦妥善為之。	配合本法施行細則第十二條第二項第六款規定，就資料安全管理事項，明定護理機構應採行之資料安全管理措施，以確保個人資料安全維護。

條文	說明
六、訂定紙本資料之銷毀程序;電腦、自動化機器或其他儲存媒介物需報廢或轉作其他用途時,應採取適當防範措施,以避免洩漏個人資料。	
第十六條　護理機構為維護所保有個人資料之安全,應採取下列人員管理措施: 一、檢視各相關業務流程涉及蒐集、處理及利用個人資料之負責人員。 二、依據作業之需要,適度設定所屬人員不同之權限並控管其接觸個人資料,並定期確認權限內容之適當及必要性。 三、要求所屬人員妥善保管個人資料之儲存媒介物,並與所屬人員約定保管及保密義務。 四、所屬人員離職或完成受指派工作後,應將其執行業務所持有之個人資料辦理交接,不得私自持有複製物而繼續使用該個人資料,並要求其返還個人資料之載體,銷毀或刪除因執行業務儲存而持有之個人資料。	配合本法施行細則第十二條第二項第六款規定,就人員管理事項,明定護理機構應採行之人員管理措施,以確保個人資料安全維護。
第十七條　護理機構保有之個人資料存在於紙本及資訊儲存媒介物,應採取下列設備安全管理措施: 一、依據業務特性、內容及需求,實施適當進出管制。 二、依媒介物之特性、使用方式及其環境,建置適當保護設備或技術。 三、針對不同作業環境,加強天然災害及其他意外災害之防護,並建置必要之防災設備。	一、配合本法施行細則第十二條第二項第八款規定,就設備安全管理事項,明定護理機構應採行之環境與設備安全管理措施,以確保個人資料安全維護。 二、本條所稱資訊儲存媒介物,係指磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒介物者。
第四章　個人資料之安全稽核、記錄保	章名

條文	說明
存及持續改善機制	
第十八條　護理機構應採行適當措施，採取個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存機制，以供必要時說明其所定維護計畫之執行情況；其相關紀錄之保存期限，至少為七年。	一、配合本法施行細則第十二條第二項第十款規定有關使用紀錄、軌跡資料及證據保存事項，明定護理機構應留存相關軌跡紀錄，以明確個人資料使用歷程情形，並避免爭議。 二、另按本法第三十條有關損害賠償請求權，應自損害發生時起五年內行使。為避免發生損害請求賠償時，相關紀錄已遭護理機構提前銷毀，爰參考紀錄保存期限，明定應至少留存七年。
第十九條　護理機構於業務終止後，其保有之個人資料應依下列方式處理及記錄： 一、銷毀：記錄銷毀之方法、時間、地點及證明銷毀之方式。 二、移轉：記錄移轉之原因、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：記錄其方法、時間或地點。 前項之相關證據及紀錄，應至少留存五年。但法令另有規定者，不在此限。	一、配合本法施行細則第十二條第二項第十款規定有關使用紀錄、軌跡資料及證據保存事項，明定護理機構應留存相關軌跡紀錄，以明確個人資料使用歷程情形，並避免爭議。 二、另按本法第三十條有關損害賠償請求權，應自損害發生時起五年內行使。為避免發生損害請求賠償時，相關紀錄已遭護理機構提前銷毀，爰明定至少留存五年，但法令另有規定者，不在此限。
第二十條　為確保本計畫之落實，護理機構應依其業務規模及特性，衡酌經營資源之合理分配，訂定適當之個人資料安全稽核機制，定期或不定期查察是否落實執行本計畫等相關事項。	配合本法施行細則第十二條第二項第九款規定有關資料安全稽核機制事項，明定發行機構應訂定個人資料安全稽核機制，以利落實執行相關規範。
第二十一條　護理機構應參酌執行業務現況、社會輿情、技術發展、法令變化等因素，檢視所定維護計畫	配合本法施行細則第十二條第二項第十一款規定有關個人資料安全維護之整體持續改善事項，明定發行機構應參

條文	說明
是否合宜，必要時予以修正。	酌執行業務現況、社會輿情、技術發展、法令變化等因素，適時檢討修正本計畫，俾利持續改善個人資料安全維護運作機制。
第五章　附則	章名
第二十二條　本辦法自發布日後一年施行。	一、本辦法施行日期。 二、考量本辦法規範之護理機構目前數量眾多，為利其因應調適，爰給予一年之緩衝期，以利護理機構配合依規定訂定計畫及建立個人資料檔案安全維護相關措施。