長期照顧服務機構個人資料檔案安全維護計畫實施辦法草案

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。	本辦法之授權依據。
第二條　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。	本辦法之主管機關。
第三條　本辦法用詞，定義如下： 一、長期照顧服務機構(以下簡稱長照機構)：指公立長照機構以外，依長期照顧服務法(以下簡稱長服法)第二十一條所定機構住宿式服務類長照機構及設有機構住宿式服務之綜合式服務類長照機構。 二、專責人員：指由長照機構指定，負責個人資料檔案安全維護計畫(以下簡稱安全維護計畫)訂定及執行之人員。 三、所屬人員：指長照機構執行業務過程中接觸個人資料之人員。 四、查核人員：指由長照機構指定，負責稽核安全維護計畫執行情形及成效之人員。 前項第二款專責人員與第四款查核人員，不得為同一人。	一、本辦法之適用對象為私立機構住宿式服務類長照機構及設有機構住宿式服務之綜合式長照機構；公立長照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，爰於第一項第一款明定。 二、為使安全維護計畫有效運作，爰於第一項第二款至第四款明定個人資料安全維護相關人員，包括專責人員、所屬人員及查核人員，並規定其定義。 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。
第四條　長照機構應依本辦法規定訂定安全維護計畫，並報經直轄市、縣（市）主管機關備查。 前項安全維護計畫，應載明下列事項： 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、資料安全管理及人員管理。 四、事故之預防、通報及應變機制。	考量長照機構規模不一，經營主體與型態未盡相同，尚難作統一規範，且參照本法施行細則第十二條第二項規定意旨，所採行之安全措施與所欲達成之個人資料保護目的間，以具有適當比例為原則，爰明定長照機構訂定安全維護計畫時，應視其規模、特性、保有個人資料之性質、方法及數量等事項，訂定適宜並符合比例原則之計畫項目。

五、設備安全管理。 六、資料安全稽核機制。 七、使用紀錄、軌跡資料及證據保存。 八、業務終止後個人資料處理方法。 九、個人資料安全維護之整體持續改善方案。	
第五條　長照機構執行業務，以資通系統蒐集、處理或利用其當事人之個人資料，且許可床數逾二百床者，應採取下列資訊安全措施: 一、使用者身分確認及保護機制。 二、個人資料顯示之隱碼機制。 三、網際網路傳輸之安全加密機制。 四、應用系統於開發、上線、維護及其他階段軟體驗證與確認程序。 五、個人資料檔案及資料庫存取控制與保護監控措施。 六、防止外部網路入侵對策。 七、非法或異常使用行為之監控與因應機制。 前項第六款、第七款所定措施，長照機構應定期演練及檢討改善。	一、查當事人健康管理或與家屬日常生活聯繫，實務上常透過網際網路或民間自行建置之資訊平台進行。考量網際網路對於個人資料安全之潛在風險，若有資安事件發生，床數逾二百床之長照機構影響之層面甚巨，爰明定達一定規模之長照機構應採取較嚴格之資訊安全措施，以符合實務執行之需求。 二、本條所稱資通系統，依據資通安全管理法第三條第一款，指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。
第六條　長照機構應依其業務規模及特性，衡酌經營資源之合理分配，規劃、訂定、檢討、修正安全維護措施，納入安全維護計畫，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。	適用本辦法之長照機構應配置相當資源，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　專責人員應負責規劃、訂定、修正、執行安全維護計畫，及業務終止後個人資料處理方法與其他相關事項，並定期向長照機構提出報告。	依本法施行細則第十二條規定，本法第二十七條第一項所稱適當之安全措施，指為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，得包括配置管理之人員及相當資源，為有效訂定與執行安全維護計畫，長照機構應指定專人辦理有關事項，爰明定專責人員之任務。
第八條　長照機構訂定第四條第二項第一款個人資料蒐集、處理及利用之內部管理程序、第二款個人資料之範圍及項目時，應包括下列	一、長照機構應依本法第十九條及第二十條蒐集、處理及利用個人資料，爰為第一項及第二項規定。

事項： 一、個人資料之蒐集、處理，應符合本法第十九條規定。 二、個人資料之利用，應符合本法第二十條規定。 三、定期檢視所保有之個人資料，發現有非屬特定目的範圍內之個人資料，或特定目的消失、期限屆至而無保存必要者，應予刪除、銷毀、停止蒐集、處理、利用或為其他適當之處置。 四、個人資料之傳輸，應採取必要保護措施，避免洩漏。 五、個人資料之蒐集，應遵守本法第八條及第九條規定辦理，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項。	二、為維護當事人權益，爰於第三款明定長照機構對個人資料應定期檢視，並為適當處置。 三、第四款明定長照機構如有傳輸個人資料之情事，應採取必要保護措施，避免洩漏。 四、第五款長照機構依本法第八條及第九條規定，如有例外免告知事由者，應確認該事由是否符合規定；另規定長照機構應採取適當告知方式履行告知義務。
第九條 長照機構將當事人個人資料為國際傳輸前，應檢視是否受中央主管機關限制，並告知當事人擬傳輸之國家或區域。	依本法第二十一條規定：「非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：(一)涉及國家重大利益。(二)國際條約或協定有特別規定。(三)接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。(四)以迂迴方法向第三國（地區）傳輸個人資料規避本法。」，長照機構將當事人個人資料為國際傳輸前，應先檢視中央主管機關對於個人資料國際傳輸之限制，且遵循之，並且於國際傳輸前，應履行告知當事人之義務。
第十條 長照機構訂定第四條第二項第三款資料安全管理及人員管理之措施，應包括下列事項： 一、依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，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。	長照機構與所屬人員，不論是何種法律關係，長照機構都應避免其保管或蒐集、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。

四、所屬人員離職時取消其識別碼，並要求將執行業務所持有之紙本及儲存媒介物之個人資料辦理交接，不得攜離使用，及簽訂保密切結書。	
第十一條　長照機構訂定第四條第二項第四款事故之預防、通報及應變機制，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，並於發現個資外洩後七十二小時內，以適當方式通知當事人或其法定代理人，並通報直轄市、縣(市)主管機關及通知中央主管機關。 三、研議改進措施，避免事故再度發生。 長照機構於發生個人資料被竊取、洩漏、竄改或其他侵害事故時，應依前項事故之預防、通報及應變機制迅速處理，保護當事人之權益。 長照機構發生前項事故者，主管機關得依本法第二十二條第一項規定進入檢查、命相關人員為必要之說明、配合措施或提供相關證明資料，並視檢查結果為後續處置。 第一項第一款通報紀錄格式如附表。	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，爰於第一項明定長照機構在安全維護計畫中應訂定應變機制。 二、第二項明定發生個人資料外洩時，應依第一項事故應變機制迅速處理，以保護當事人之權益。 三、第三項明定長照機構發生個人資料侵害事故，主管機關得依本法第二十二條規定辦理檢查，並視檢查結果為後續處置。
第十二條　長照機構訂定第四條第二項第五款設備安全管理之措施，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、紙本及電子資料之銷毀程序。 四、電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。	為確保長照機構所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，爰為本條規定。
第十三條　查核人員應依第四條第二項第六款	為確保個人資料維護安全措施發生效能，明定

規定，定期或不定期稽核安全維護計畫之執行情形，並出具稽核報告，必要時向長照機構提出改善計畫。	長照機構應訂定個人資料檔案安全維護稽核機制，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，爰規定查核人員應向長照機構提出稽核報告或改善計畫，促使長照機構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。
第十四條　長照機構訂定第四條第二項第七款使用紀錄、軌跡資料及證據保存之措施，應包括下列事項： 一、留存個人資料使用紀錄。 二、留存自動化機器設備之軌跡資料或其他相關之證據資料。 三、前二款紀錄及資料證據之保存措施。	長照機構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，作為日後發生問題時提供說明佐證，以釐清法律責任。
第十五條　長照機構訂定第四條第二項第八款業務終止後個人資料處理方法之措施，應包括下列事項： 一、銷毀：方法、時間、地點及證明銷毀之方式。 二、移轉：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、刪除、停止處理或利用：方法、時間或地點。 前項措施應製作紀錄，並至少留存五年。	一、長照機構於業務終止後，不得再繼續使用其所保有之個人資料檔案，並應作妥善處置。長照機構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、刪除或其他方式處理，且應記錄處理之方法、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。 二、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。
第十六條　長照機構訂定第四條第二項第九款個人資料安全維護之整體持續改善方案，應參酌安全維護計畫執行狀況、技術發展、法令修正或其他因素，檢視所定安全維護計畫之合宜性，必要時應予修正。	長照機構應參酌相關因素，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。

第十七條　長照機構應於本辦法發布施行後一年內，完成安全維護計畫之訂定及實施。主管機關得定期派員檢查。	長照機構之安全維護計畫應於本辦法發布施行後一年內完成訂定及實施，且主管機關得派員檢查。
第十八條　本辦法自發布日施行。	本辦法之施行日期。

附表

<table>
<tr><td colspan="3">個人資料侵害事故通報紀錄表</td></tr>
<tr><td>長期照顧服務機構名稱</td><td colspan="2" rowspan="2">通報時間：　年　月　日　時　分
通報人：　　簽名（蓋章） 職稱
電話：
Email：
地址：</td></tr>
<tr><td>通報機關</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事件發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個資侵害之總筆數（大約）
_____ 筆</td></tr>
<tr><td>□一般個資_____ 筆
□特種個資_____ 筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬通知當事人之
時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個資
外洩後七十二小時
通報</td><td colspan="2">□是　　□否，理由</td></tr>
</table>