精神復健機構個人資料檔案安全維護計畫實施辦法部分條文修正草案總說明

精神復健機構個人資料檔案安全維護計畫實施辦法（以下簡稱本辦法），於一百零九年五月十九日訂定發布全文十八條。茲配合國家發展委員會一百十年二月三日「行政機關落實個人資料保護執行聯繫會議」第一次會議決議及行政院一百十年八月十一日訂定發布「行政院及所屬各機關落實個人資料保護聯繫作業要點」規定，強化精神復健機構對個人資料檔案之安全維護及資安標準規範，爰擬具本辦法部分條文修正草案，其修正要點如下：

一、精神復健機構傳輸個人資料至境外，應告知當事人或法定代理人並取得書面同意。（修正條文第八條）

二、精神復健機構使用資通訊系統蒐集、處理或利用個人資料時，應有使用者身分確認保護機制、網際網路傳輸安全加密機制、個人資料檔案及資料庫之存取控制與保護監控等資訊安全措施。（修正條文第九條）

三、精神復健機構發生個人資料事故時，應於發現時起七十二小時內通報當地直轄市或縣（市）政府及通知中央主管機關，俾利直轄市或縣（市）政府得依個人資料保護法第二十二條至第二十五條規定，為適當之監督管理措施。（修正條文第十一條）

四、增訂公立精神復健機構及可收治服務對象二百人以下私立精神復健機構準用個人資料跨境傳輸及個人資料重大事故通報規定。（修正條文第十七條之一）

精神復健機構個人資料檔案安全維護計畫實施辦法部分條文修正草案條文對照表

修正條文	現行條文	說明
第八條　精神復健機構蒐集個人資料時，應符合前條第一項所定之類別及範圍。 精神復健機構於傳輸個人資料時，應採取必要保護措施，避免洩漏。 精神復健機構將服務對象之個人資料為國際傳輸前，應檢視是否受中央主管機關限制，並告知當事人或其法定代理人有關個人資料之範圍及擬傳輸之國家或區域，及取得書面同意。	第八條　精神復健機構蒐集個人資料時，應符合前條第一項所定之類別及範圍。 精神復健機構於傳輸個人資料時，應採取必要保護措施，避免洩漏。	一、依個人資料保護法第六條、第二十七條及一百十年八月十九日衛生福利部「研商非公務機關個人資料國際傳輸之限制」會議決議，機構將個人資料作國際傳輸者，應告知當事人或其法定代理人個人資料所欲傳輸之區域，並取得書面同意，爰為第三項規定。 二、諸如精神復健機構服務對象個人資料傳輸至雲端資料儲存或處理服務，其伺服器位於我國境外者，或傳輸至我國境外之長期照顧服務或醫療機構，均應有第三項之適用。
第九條　精神復健機構蒐集之服務對象個人資料，應依本法第八條及第九條、精神復健機構設置及管理辦法第十一條及第十二條規定辦理，並依直接蒐集或間接蒐集，分別訂定告知方式、內容及其注意事項。 精神復健機構使用資通訊系統蒐集、處理或利用服務對象個人資料	第九條　精神復健機構蒐集個人資料時，應依精神復健機構設置及管理辦法第十一條及第十二條規定辦理，並依直接蒐集或間接蒐集，分別訂定告知方式、內容及其注意事項。	一、為明確蒐集個人資料之依據，爰修正第一項。 二、為落實個人資料之保護，依行政院一百十年八月十一日訂定發布「行政院及所屬各機關落實個人資料保護聯繫作業要點」第四點規定，爰增訂第二項。 三、隨網路資訊發達與科

時，應採取下列資料安全管理措施： 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、個人資料檔案及資料庫之存取控制與保護監控措施。 五、外部網路入侵防範對策。 六、非法或異常使用行為之監控與因應機制。 前項第五款及第六款所定措施，應定期演練及檢討改善。		技之進步，可能發生個人資料於網路遭非法入侵或異常使用行為損害情形，爰增訂第三項，明定針對前項第五款及第六款所定措施，精神復健機構應定期進行演練及檢討改善。
第十一條　精神復健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，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。 四、發生事故者，應於發現時起七十二小時內，通報直轄市或縣（市）政府及通知中央主管機關。	第十一條　精神復健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，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。 精神復健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	配合國家發展委員會一百十年二月三日「行政機關落實個人資料保護執行聯繫會議」第一次會議決議，發生事故者，機構應於發現時起七十二小時內通報地方目的事業主管機關及通知中央主管機關，爰增訂第一項第四款。另依該次會議國家發展委員會所示個人資料事故通報格式參考範本，並參考「內政部指定移民業務機構個人資料檔案安全維護管理辦法」第十三條及「醫療器材批發零售業個人資料檔案安全維護計畫實施辦法」第十七條所定書面通報格式，於第三項增訂通報格式如附表。

精神復健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。 第一項第四款通報紀錄格式如附表。	理，保護當事人之權益。	
第十七條之一　第八條第三項、第十一條第一項第四款及第三項規定，於公立精神復健機構及可收治服務對象二百人以下私立精神復健機構，準用之。		一、本條新增。 二、公立醫院所持有資訊均屬政府資訊，又其亦行使部分公權力行為，爰公立精神復健機構係比照本法之「公務機關」規定，而可收治服務對象二百人以下私立精神復健機構依其規模與行政量能等實務面考量，尚毋須逐一訂定個人資料檔案安全維護計畫，故上開二類機構非屬第三條第一項第一款定義所稱精神復健機構；惟有關個人資料跨境傳輸及個人資料事故通報之規範，宜有統一規定，為使該等機構有所依循，爰增訂本條。

附表

<table>
<tr><td colspan="3">精神復健機構個人資料事故通報及紀錄表</td></tr>
<tr><td>精神復健機構名稱

通報機關</td><td colspan="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>發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">發生種類</td><td rowspan="2">□竊取
□竄改
□毀損
□滅失
□洩漏
□其他侵害情形</td><td>個人資料侵害之總筆數
（大約）</td></tr>
<tr><td>□一般個人資料　　筆
□特種個人資料　　筆</td></tr>
<tr><td>發生原因及摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料侵害可能結果</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>是否於發現個人資料外洩後七十二小時內通報</td><td colspan="2">□是　□否，理由：</td></tr>
<tr><td colspan="3">備註：特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料；一般個人資料，指特種個人資料以外之個人資料。</td></tr>
</table>