非輻射電子醫療器材設備製造業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。」，爰訂定非輻射電子醫療器材設備製造業個人資料檔案安全維護計畫實施辦法(以下簡稱本辦法)，全文共二十三條，其要點如下：

一、本辦法訂定之法律授權依據。(第一條)

二、本辦法之主管機關。(第二條)

三、本辦法之用詞定義。(第三條)

四、非輻射電子醫療器材設備製造業者應訂定個人資料檔案安全維護計畫。(第四條)

五、非輻射電子醫療器材設備製造業者應落實個人資料檔案之安全維護及管理。(第五條)

六、非輻射電子醫療器材設備製造業者應完成安全維護計畫訂定之期程及主管機關得派員檢查該計畫。(第六條)

七、非輻射電子醫療器材設備製造業者應指定專責人員負責個人資料檔案安全維護之相關任務。(第七條)

八、非輻射電子醫療器材設備製造業者所保有之個人資料，經定期檢視，應予刪除、銷毀或停止蒐集、處理及利用之情形。(第八條)

九、非輻射電子醫療器材設備製造業者蒐集及傳輸個人資料時應符合之規定。(第九條)

十、非輻射電子醫療器材設備製造業者蒐集個人資料應遵守之告知義務。(第十條)

十一、非輻射電子醫療器材設備製造業者將個人資料為國際傳輸前

應符合之規定。(第十一條)

十二、非輻射電子醫療器材設備製造業者利用個人資料為宣傳、推廣或行銷時應符合本法之規定，並提供當事人或法定代理人拒絕行銷之機制。(第十二條)

十三、非輻射電子醫療器材設備製造業者委託他人蒐集、處理或利用個人資料時，應對受託人為適當之監督。(第十三條)

十四、非輻射電子醫療器材設備製造業者對於當事人行使本法第三條規定之權利，得採行之辦理方式。(第十四條)

十五、非輻射電子醫療器材設備製造業者應對資料安全管理人員採取之措施。(第十五條)

十六、非輻射電子醫療器材設備製造業者提供電子商務服務，應採取之安全措施。(第十六條)

十七、非輻射電子醫療器材設備製造業者應訂定個人資料侵害事故發生之預防、通報及應變機制。(第十七條)

十八、非輻射電子醫療器材設備製造業者應對保有之個人資料設置必要之安全設備及採取必要之防護措施。(第十八條)

十九、非輻射電子醫療器材設備製造業者應訂定個人資料檔案安全維護稽核機制。(第十九條)

二十、非輻射電子醫療器材設備製造業者應留存個人資料使用紀錄、自動化機器設備之軌跡資料。(第二十條)

二十一、非輻射電子醫療器材設備製造業者業務終止後，對其保有之個人資料之處理方法及留存紀錄。(第二十一條)

二十二、非輻射電子醫療器材設備製造業者應檢視所定安全維護計畫之合宜性，以持續改進個人資料保護機制。(第二十二條)

非輻射電子醫療器材設備製造業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。	依個人資料保護法(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。」，爰明定本辦法之法源依據。
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、非輻射電子醫療器材設備製造業者(以下簡稱業者)：指工廠登記之產業類別為輻射及電子醫學設備製造業，製造非可發生游離輻射電子醫療器材設備，依醫療器材管理法第十三條規定核准登記，且資本額新臺幣三千萬元以上，並有招募會員或可取得交易對象個人資料之醫療器材製造業者。 二、專責人員：指由業者指定，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：指業者執行業務之過程中接觸個人資料之人員。 四、查核人員：指由業者指定，負責稽核安全維護計畫執行情形及成	一、本辦法之適用對象。 二、依行政院主計總處行業統計分類(第十一版修正)，代碼為 276 輻射及電子醫學設備製造業，其中屬製造可發生游離輻射設備者，係適用「游離輻射設備製造業個人資料檔案安全維護管理辦法」之規範，爰明定本辦法適用對象為非輻射電子醫療器材設備製造業者。 三、業者資本額新臺幣三千萬元以上者，其個人資料管理之風險因規模而升高，如又有以會員制或其他方式取得個人資料者，即有特別予以規範之必要，爰明定納入本辦法之列管範圍。 四、為使安全維護計畫有效運作，爰於第一項第二款至第四款規範個人資料安全維護相關人員，包括專責人員、查核人員及所屬人員，並規定其

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。	定義。 五、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　業者應依本辦法規定訂定安全維護計畫，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。 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。	考量業者規模不一，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，爰由業者自行訂定安全維護計畫，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。
第五條　業者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、檢討及修正安全維護措施，並納入安全維護計畫，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。	適用本辦法之業者應配置相當資源，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，防止個人資料被竊竊取、竄改、毀損、滅失或洩漏。
第六條　業者應於本辦法發布施行後六個月內，完成安全維護計畫之訂定。 業者應保存前項安全維護計畫；主管機關得定期派員檢查。	一、第一項明定業者之安全維護計畫應於本辦法發布施行後，六個月內完成訂定。 二、第二項明定前項安全維護計畫應妥善保存，主管機關得派員檢查。
第七條　專責人員負責規劃、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，並定期向業者提出報告。	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，為有效訂定與執行本計畫，業者應指定

	專人辦理有關事項，爰明定專責人員之任務。
第八條　業者訂定第四條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。 業者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、期限屆至而無保存必要者，應予刪除、銷毀、停止蒐集、處理、利用或其他適當之處置。	一、業者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，爰於第一項明定業者應依蒐集之特定目的，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查其現況。 二、為維護當事人權益，爰於第二項明定業者對個人資料應定期檢視及清查，並為適當處置。
第九條　業者蒐集個人資料時，應符合前條第一項所定之類別及範圍。 業者於傳輸個人資料時，應採取必要保護措施，避免洩漏。	一、第一項明定業者蒐集個人資料，應符合之類別及範圍。 二、第二項明定如有傳輸個人資料之情事，應採取必要保護措施。
第十條　業者蒐集個人資料時，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。	一、業者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。 二、業者應採取適當告知方式以履行告知義務。
第十一條　業者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。	業者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規定，且遵循之，並且於國際傳輸前，應履行告知當事人之規定。
第十二條　業者依本法第二十條第一項規定利用個人資料為宣傳、推廣或行銷時，應明確告知當事人業者立案名稱及個人資料來源。 業者首次利用個人資料為宣傳、推廣或行銷時，應提供當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷之方式，並支付所需費用；當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷者，應立即停止利用，並周知所屬人員。	一、依本法第八條第一項規定，非公務機關向當事人蒐集個人資料時，應明確告知當事人非公務機關之名稱，以利當事人知悉向其為宣導、推廣或行銷之主體。爰於第一項明定業者利用個人資料為宣傳、推廣或行銷時，應明確告知當事人之事項。 二、為利當事人或其法定代理人查知利用個人資料行銷，是否符合本法第二十條第二項及第三項規定，爰於第二項明定業者應提供當事人或其

	法定代理人表示拒絕接受宣傳、推廣或行銷之方式。
第十三條　業者委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定對受託人為適當之監督，並於委託契約或相關文件中，明確約定其內容。	業者將個人資料之蒐集、處理或利用委託他人為之，應對受託人為適當之監督，以使資料之蒐集、處理或利用符合法令之要求。
第十四條　業者於當事人或其法定代理人行使本法第三條規定之權利時，得採取下列方式辦理： 一、提供聯絡窗口及聯絡方式。 二、確認為個人資料當事人本人、法定代理人，或經其委託之人。 三、有本法第十條但書、第十一條第二項但書或第三項但書，得拒絕當事人或其法定代理人行使權利之事由者，併附理由通知當事人或其法定代理人。 四、遵守本法第十三條處理期限規定。 五、告知依本法第十四條規定得酌收必要成本費用。	業者對於當事人或其法定代理人行使本法第三條規定之權利，應遵守本法第三條、第十條、第十一條、第十三條及第十四條規定，採取相關方式辦理，以保障當事人權利。
第十五條　業者訂定第四條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。 四、取消所屬人員離職時原在職之識別碼，並要求將執行業務所持有	業者與所屬人員，不論是何種法律關係，業者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。

他人個人資料辦理交接，不得攜離使用。	
第十六條　業者提供電子商務服務系統，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、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、非法或異常使用系統之監控與因應機制。 前項所稱電子商務，指透過網際網路進行商品或服務之廣告、行銷、供應、訂購、遞送或其他商業交易活動。 第一項第五款對策及第六款機制，應定期演練及檢討改善。	一、為強化資安標準規範，爰於第一項明定業者提供電子商務服務系統，應採行之資訊安全措施，以落實民眾個人資料安全之保障。 二、第二項界定電子商務服務範圍。 三、第三項明定業者應定期演練第一項第五款及第六款所定措施，以及時發現問題並檢討改善。
第十七條　業者訂定第四條第四款事故之預防、通報及應變機制，應包括下列事項： 一、採取適當措施，控制事故對當事人造成之損害，並於發現事故時起七十二小時內，通報直轄市、縣(市)主管機關及通知中央主管機關。 二、查明事故發生原因及損害狀況，並通知當事人或其法定代理人。 三、檢討缺失，並訂定預防及改進措施，避免事故再度發生。 業者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。 業者發生前項事故者，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。	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，爰於第一項明定業者在安全維護計畫中應訂定侵害事故發生之應變機制。 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、第三項明定業者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之規定。 四、第四項明定個人資料侵害事故通報紀錄表格式。

第一項第一款通報紀錄格式如附表。	
第十八條　業者訂定第四條第五款設備安全管理措施，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；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。	為確保業者所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，業者應視其規模、業務性質、資料儲存媒介物及其數量等，對所保有之個人資料，設置必要之安全設備及採取必要之防護措施。
第十九條　查核人員應依第四條第六款規定，定期或不定期稽核安全維護計畫之執行情形及成效，並將稽核結果，向業者提出報告。	為確保個人資料維護安全措施發生效能，業者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，除能證明已盡防止個人資料遭侵害之義務者外，應受同一額度罰鍰，爰規定查核人員應向業者提出稽核結果報告，促使業者得據以監督安全維護計畫之執行事項，證明已盡防止個人資料遭侵害之義務。
第二十條　業者訂定第四條第七款使用紀錄、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。	業者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，作為日後發生問題之佐證，以釐清法律責任。
第二十一條　業者訂定第四條第八款業務終止後，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	一、業者於業務終止後，自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。爰終止業務之業者，應視其終止業務之原因，將所保有之個人資料予以銷毀、刪除、移轉或其他停止處理或利用等方式處理，

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。	爰為第一項規定，並於處理過程中，保存處理方式、地點、時間、執行人員、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。
第二十二條　業者訂定第四條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。	業者應參酌相關因素，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。
第二十三條　本辦法自發布日施行。	本辦法之施行日期。

附表

個人資料侵害事故通報紀錄表

<table>
<tr><td>非輻射電子醫療器材設備製造業名稱：</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>通報機關：</td><td colspan="2"></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>