正本

檔　　號：
保存年限：

衛生福利部　函

機關地址：11558 台北市南港區忠孝東路六段488號
傳　　真：
聯絡人及電話：林盈晶02-27877528
電子郵件信箱：brenda1228@fda.gov.tw

241
新北市三重區重新路五段609巷6號3樓之3

受文者：台灣醫療暨生技器材工業同業公會

台灣醫療暨生技器材工業同業公會
收 108. 05. 17 文
檔號：108302

發文日期：中華民國108年5月16日
發文字號：衛授食字第1081603178號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：「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」草案，業經本部於中華民國108年5月16日以衛授食字第1081603106號公告預告，請查照並轉知所屬。

說明：

一、旨揭公告請至行政院公報資訊網、本部網站「衛生福利法規檢索系統」下「法規草案」網頁、本部食品藥物管理署網站「公告資訊」下「本署公告」網頁及國家發展委員會「公共政策網路參與平臺—眾開講」網頁 (https://join.gov.tw/policies/) 自行下載。

二、對公告內容有任何意見者，請於本草案刊登前揭網站之隔日起60日內陳述意見或洽詢：

(一)承辦單位：衛生福利部食品藥物管理署
(二)地址：台北市南港區昆陽街161-2號
(三)電話：02-2787-7528
(四)傳真：02-3322-9492
(五)電子郵件：brenda1228@fda.gov.tw

正本：台灣醫療暨生技器材工業同業公會(不含附件)
副本：衛生福利部法規會

部長陳時中

衛生福利部公告

中華民國 108 年 5 月 16 日
衛授食字第 1081603106 號

主　　旨：預告訂定「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」草案。

依　　據：行政程序法第一百五十四條第一項。

公告事項：

一、訂定機關：衛生福利部。

二、訂定依據：個人資料保護法第二十七條第三項。

三、「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」草案總說明及逐條說明如附件。本案另載於行政院公報資訊網、本部網站「衛生福利法規檢索系統」下「法規草案」網頁、本部食品藥物管理署網站「公告資訊」下「本署公告」網頁及國家發展委員會「公共政策網路參與平臺－眾開講」網頁（https://join.gov.tw/policies/）。

四、對於公告內容有任何意見或修正建議者，請於本公告刊登公報之隔日起 60 日內，至前揭「衛生福利法規檢索系統」或「公共政策網路參與平臺－眾開講」網頁陳述意見或洽詢：

(一) 承辦單位：衛生福利部食品藥物管理署

(二) 地址：台北市南港區昆陽街 161-2 號

(三) 電話：02-2787-7528

(四) 傳真：02-3322-9492

(五) 電子郵件：brenda1228@fda.gov.tw

部　　長　陳時中

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草案總說明

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。」。

鑑於近期個人資料外洩事件頻傳,加強個人資料保護之需求日益殷切。為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，擬具「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」(以下簡稱本辦法)，其要點如次：

一、法源依據。(草案第一條)

二、本辦法之主管機關。(草案第二條)

三、本辦法之用語定義。(草案第三條)

四、醫療器材批發零售業者應訂定安全維護計畫。(草案第四條)

五、醫療器材批發零售業者應落實個人資料檔案之安全維護及管理。(草案第五條)

六、醫療器材批發零售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。(草案第六條)

七、醫療器材批發零售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。(草案第七條)

八、醫療器材批發零售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。(草案第八條)

九、醫療器材批發零售業者蒐集及傳輸個人資料時應符合之規定。(草案第九條)

十、醫療器材批發零售業者蒐集個人資料應遵守之告知義務。(草案第十條)

十一、醫療器材批發零售業者利用個人資料為宣傳、推廣或行銷時之應符合本法之規定，並提供當事人或法定代理人拒絕行銷之機制。(草案第十一條)

十二、醫療器材批發零售業者委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督。（草案第十二條）

十三、醫療器材批發零售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。（草案第十三條）

十四、醫療器材批發零售業者應訂定應變機制。（草案第十四條）

十五、醫療器材批發零售業者應設置必要之安全設備及採取必要之防護措施。（草案第十五條）

十六、醫療器材批發零售業者應對其所屬人員採取之措施。（草案第十六條）

十七、醫療器材批發零售業者應訂定個人資料檔案安全維護查核機制。（草案第十七條）

十八、醫療器材批發零售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。（草案第十八條）

十九、醫療器材批發零售業者應定期或不定期對其所屬人員施以個人資料保護相關法令規定之教育訓練或宣導。（草案第十九條）

二十、醫療器材批發零售業者業務終止後，對其保有之個人資料之處理方法及留存紀錄。（草案第二十條）

二十一、醫療器材批發零售業者應檢視所定計畫之合宜性，以持續改進個人資料保護機制。（草案第二十一條）

二十二、本辦法施行日。（草案第二十二條）

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。	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。	明定本辦法之主管機關。
第三條　本辦法用詞，定義如下： 一、醫療器材批發零售業者：指依藥事法第二十七條之規定核准登記，且資本額超過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販賣業者。 二、專責人員：指由醫療器材批發零售業者指定，負責個人資料檔案安全維護計畫(以下簡稱安全維護計畫)訂定及執行人員。 三、所屬人員：指醫療器材批發零售業者執行業務之過程，接觸個人資料之人員。 四、查核人員：指由醫療器材批發零售業者指定，負責評核安全維護計畫執行情形及成效之人	一、明定本辦法之適用對象。 二、醫療器材批發零售業者如以公司或商號形式為事業主體，或經營工廠者，其接觸個人資料之層面均較複雜；該業者資本額若達新臺幣三千萬元以上，則其個人資料管理之風險亦因規模而升高，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。 三、為使安全維護計畫有效運作，爰於第一項明定個人資料安全維護相關人員，包括個人資料專責人員、查核人員及所屬人員，並規定所屬人員之定義。 四、為確保查核制度獨立及確實執行，爰於第二項明定個人資料專責人員與查核人員不得為同一人。

員。 前項第二款專責人員與第四款查核人員，不得為同一人。	
第四條　醫療器材批發零售業者應依本辦法規定訂定安全維護計畫。 前項安全維護計畫，應包括下列項目： 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。	考量醫療器材批發零售業者規模不一，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，爰明定醫療器材批發零售業者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。
第五條　醫療器材批發零售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、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　醫療器材批發零售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。 醫療器材批發零售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、第一項明定醫療器材批發零售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	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、

關事項，並定期向醫療器材批發零售業者提出報告。	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，醫療器材批發零售業者應指定專人辦理有關事項，爰明定醫療器材批發零售業者應指定專責人員，負責個人資料檔案安全維護，並明定專責人員之任務。
第八條　醫療器材批發零售業者應依第四條第二項第一款、第二款規定，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。 醫療器材批發零售業者經定期檢視，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、期限屆滿而無保存必要者，應依第四條第二項第一款規定，刪除、銷毀、停止蒐集、處理、利用或其他適當之處置。	一、醫療器材批發零售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，爰於第一項明定醫療器材批發零售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，爰於第二項明定醫療器材批發零售業者對個人資料應定期檢視及清查，並為適當處置。
第九條　醫療器材批發零售業者於蒐集個人資料時，應檢視是否符合前條第一項所定之類別及範圍。 醫療器材批發零售業者於傳輸個人資料時，應採取必要保護措施，避免洩漏。	一、第一項明定醫療器材批發零售業者蒐集個人資料，應符合前條第一項所定之類別及範圍。 二、第二項明定醫療器材批發零售業者如有傳輸個人資料之情事，應採取必要保護措施，避免洩漏。
第十條　醫療器材批發零售業者於蒐集個人資料時，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，要求所屬人員確實辦理。	一、明定醫療器材批發零售業者依本法第八條及第九條規定，如有例外免告知事由者，並應確認該事由是否符合規定。 二、明定業者應採取適當告知方式以履行告知義務。
第十一條　醫療器材批發零售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，應明確告知當事人醫療器材批發零售業	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、

者立案名稱及個人資料來源。 醫療器材批發零售業者於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，應立即停止利用其個人資料宣傳、推廣或行銷，並周知所屬人員。	推廣或行銷之主體。爰於第一項明定醫療器材批發零售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，爰於第二項明定醫療器材批發零售業者應提供當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷之方式及拒絕效果。
第十二條　醫療器材批發零售業者委託他人蒐集、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，對受託者為適當之監督，並明確約定相關監督事項及方式。	明定醫療器材批發零售業者將個人資料之蒐集、處理或利用委託他人為之，應對受託者為適當之監督，以使資料之蒐集、處理或利用符合法令之要求。
第十三條　醫療器材批發零售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、確認是否為資料當事人之本人或其法定代理人，或經其委託。 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，一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、告知是否依本法第十四條規定酌收必要費用。	明定醫療器材批發零售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。
第十四條 醫療器材批發零售業者應依第四條第二項第四款規定訂定應變機制，於發生個人資料被竊取、洩漏、竄改或其他侵害事故	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

時，迅速處理，以保護當事人之權益。 醫療器材批發零售業者執行前項應變機制，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及文件書表格式，由直轄市、縣(市)主管機關定之。	法定代理人，爰於第一項明定醫療器材批發零售業者在安全維護計畫中應訂定應變機制。 二、第二項明定前項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　醫療器材批發零售業者對所保有之個人資料檔案，應依據第四條第二項第五款規定設置必要之安全設備及採取必要之防護措施。 前項安全設備或防護措施，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，配置安全防護系統或加密機制。 三、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。	一、為確保醫療器材批發零售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，業者得視其規模、業務性質、資料儲存媒介物及其數量等，爰於第一項明定，醫療器材批發零售業者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。

第十六條　醫療器材批發零售業者為確實保護個人資料之安全，應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、所屬人員離職時取消其識別碼，並應要求將執行業務所持有之個人資料(包括紙本及儲存媒介物)辦理交接，不得攜離使用，並應簽訂保密切結書。	醫療器材批發零售業者與所屬人員，不論是何種法律關係，醫療器材批發零售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。
第十七條 查核人員應依第四條第二項第六款規定，定期或不定期評核安全維護計畫之執行情形及成效，並將評核結果，向醫療器材批發零售業者提出報告。	為確保個人資料維護安全措施發生效能，明定醫療器材批發零售業者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，爰規定向業者提出檢查結果報告，促使業者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。
第十八條　醫療器材批發零售業者應依第四條第二項第七款規定，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，以供必要時	醫療器材批發零售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，以供日後發生問題時提供說明佐證，以釐清其法律

說明其所定安全維護計畫之執行情形。	責任。
第十九條　醫療器材批發零售業者對於個人資料蒐集、處理及利用，應符合本法第十九條及第二十條規定，並應定期或不定期對其所屬人員施以教育訓練或認知宣導，使其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。	醫療器材批發零售業者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。
第二十條　醫療器材批發零售業者依第四條第二項第八款規定，對業務終止後，其保有個人資料之處理方式及留存紀錄如下： 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 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。	一、醫療器材批發零售業者業務於業務終止後，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。爰終止業務之醫療器材批發零售業者，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。 二、第一項明定醫療器材批發零售業者銷毀、刪除、移轉或刪除、停止處理或利用個人資料過程中，應保存處理方式、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。 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。
第二十一條　醫療器材批發零售業者應依第四條第二項第九款規定，參酌安全維護計畫執行狀況、技術發展、法令依據修正等因素，檢視所定安全維護計畫是否合宜，必要時應予修正。	明定醫療器材批發零售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。
第二十二條　本辦法自發布日施行。	本辦法之施行日期。