

社團法人台灣職業健康護理學會

個人資料檔案安全維護計畫及會務終止後個人資料處理方法

115.06.05

壹、組織及規模

- 一、組織名稱：台灣職業健康護理學會
- 二、組織型態：人民團體
- 三、會址：台中市民權路100號11樓之1
- 四、代表人：第七屆陳美滿理事長
- 五、會員及相關服務對象：包含會員、課程學員、合作單位、講師及相關聯繫對象等
- 六、業務特性：辦理職業健康護理、職場健康促進、教育訓練、學術交流及會員服務等相關業務

貳、個人資料檔案之安全維護管理措施

一、依據

依據內政部指定合作及人民團體類非公務機關個人資料檔案安全維護管理辦法規定辦理

二、目的

為防止個人資料被竊取、竄改、毀損、滅失或洩漏，爰訂定本「個人資料檔案安全維護計畫及業務終止後個人資料處理方法」（下稱本計畫及處理方法），作為學會執行個人資料管理與保護之依據。

三、管理人員及資源

- （一）學會人力包含專任或兼任行政人員、專案計畫相關人員、委辦計畫工作成員及無給職理事、監事成員。前述人員因執行學會會務、專案計畫、會員服務、教育訓練、學術活動或行政管理需要，得於授權範圍內接觸、處理或利用相關個人資料。
- （二）管理人員：
 - 1、配置人數：1 人
 - 2、職責：負責規劃、訂定、修正與執行本計畫及處理方法等相關事項，並向負責人提出報告。
- （三）個人資料保護管理政策：遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，並確實維護與管理所保有個人資料檔案安全，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- （四）學會將聯絡資訊（聯絡窗口為：秘書處，電話為：04-22257126）揭示於本學會網頁，以提供當事人表示拒絕接受行銷、個人資料事故諮詢服務及行使個人資料保護法第三條之權利聯絡使用。
- （五）資源：學會投入必要的人力、技術、資安設備、訓練及顧問輔導等資源，並視需要編列經費，以推動本計畫及處理方法。

四、個人資料之範圍

- (一) 特定目的包括會員（含會員代表）管理、教育訓練、活動辦理、學術交流、行政管理及法定義務人員名冊之內部管理。
- (二) 本計畫及處理方法所稱會員（含會員代表、理監事）個人資料指自然人之姓名、出生年月日、國民身分證統一編號、教育程度、聯絡方式、戶籍地址、執業證照、服務單位、學經歷及其他依法蒐集得以直接或間接方式識別該個人之資料。
- (三) 本計畫及處理方法所稱非會員（含停權會員、教育訓練學員）個人資料指自然人之姓名、出生年月日、國民身分證統一編號、教育程度、聯絡方式、戶籍地址、執業證照、服務單位、學經歷及其他依法蒐集得以直接或間接方式識別該個人之資料。
- (四) 本計畫及處理方法所稱會務工作人員個人資料指自然人之姓名、出生年月日、國民身分證統一編號、教育程度、聯絡方式、戶籍地址及其他得以直接或間接方式識別該個人之資料。
- (五) 本計畫及處理方法所稱專案計畫相關人員個人資料指自然人之姓名、出生年月日、國民身分證統一編號、教育程度、聯絡方式、戶籍地址、執業證照、服務單位、學經歷及其他依法蒐集得以直接或間接方式識別該個人之資料。
- (六) 依個資法第51條第1項規定，以下個人資料排除於本計畫及處理方法之外：
 - 1、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。
 - 2、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

五、風險評估及管理機制

- (一) 風險評估
 - 1、經由本學會電腦下載或外部網路入侵而外洩。
 - 2、經由接觸書面文件而外洩。
 - 3、人員及第三人故意竊取、毀損或洩漏。
 - 4、設備送修、遺失或被竊。
 - 5、互為傳輸時之外洩（包括會員間傳輸、與相關業者間傳輸等）。
 - 6、業務終止後個人資料未銷毀。
- (二) 管理機制
 - 1、定期進行網路資訊安全維護及控管。
 - 2、紙本文件應以妥適方式保管、傳遞。
 - 3、落實教育訓練及管理稽核，並監督其業務之執行。
 - 4、設備送修前或保存，應先備份或加密，避免非授權存取。
 - 5、加強對人員之管制及設備之強化管理。
 - 6、個資檔案蒐集之特定目的消失或使用期限已結束應銷毀。。

六、事故之預防、通報及應變機制

- (一) 預防

- 1、本會會務工作人員如因職務內容而須使用任一個人資料時，須於個人資料管理系統輸入個人識別帳號與密碼，並只得應用資料於相關職務內容。另如須進行個人資料文件下載，須於下載後第一時間進行資料加密，並於使用完畢後即刻永久刪除。
- 2、非承辦之會務工作人員不得存有個人資料管理系統之帳戶，如因工作內容而須暫時調閱個人資料之紙本資料時，應取得學會理事長或指定管理人員之同意。
- 3、加強會務工作人員教育訓練，並嚴加管制。

(二) 通報及應變

- 1、發現學會任一個人資料遭竊取、竄改、毀損、滅失或洩漏等安全疑慮，須立即向學會理事長通報，並調查可能發生原因，視實時狀況採取必要應對措施。
- 2、對於個人資料遭竊取或遺失之當事人，學會應以電話、電子郵件或簡訊等適當方式通知，確認當事人知悉，並提供必要之協助及諮詢服務專線。
- 3、遇有個人資料事故時，應依規定於發現後 72 小時內，以書面通報主管機關。
- 4、事故處理完畢後，應針對事故發生原因研議改進措施並留存相關紀錄。

七、個人資料蒐集、處理及利用之內部管理措施

(一) 直接向個人資料當事人蒐集個人資料時，應明確告知以下事項：

- 1、團體名稱。
- 2、蒐集目的。
- 3、利用範圍。
- 4、個人資料之類別。
- 5、個人資料利用之期間、地區、對象及方式。
- 6、當事人得依法申請查詢、閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。
- 7、當事人如須委託第三方處理個人資料，應簽訂保密與監督條款。
- 8、當事人得自由選擇是否提供相關個人資料，惟若拒絕提供或提供不完全時，可能影響會員申請、會務聯繫、活動通知或相關服務之提供。

(二) 所蒐集非由當事人提供之個人資料，應於處理或利用前向當事人告知個人資料來源及前項應告知之事項。

(三) 當事人表示請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，聯絡電話為：04-22257126。聯絡窗口及電話等資料，皆揭示於學會會址所在地及學會官方網站。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

(四) 負責保管及處理個人資料檔案之人員，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交，以利管理。

(五) 本會會務工作人員如因職務內容而須使用任一個人資料時，須於個人資料管理系統輸入個人識別帳號與密碼，並只得應用資料於相關職務內容。其中個人識別帳號及密碼應保密，不得洩漏或與他人共用。

(六) 由指定之管理人員定期查核確認所保有之個人資料現況，並界定納入本計畫

及處理方法之範圍。

- (七) 本會委託外部廠商或第三方機構蒐集、處理或利用個人資料時，當對受託者為適當之監督並與其明確約定相關監督事項。
- (八) 所蒐集之個人資料如需作特定目的以外之利用，必須先行檢視是否符合規定。
- (九) 本會因故終止會務時，原保有之個人資料，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

八、設備安全管理、資料安全管理及人員管理措施

(一) 設備安全管理

- 1、本會用來建置個人資料的電腦設備，不得直接作為公眾查詢之前端工具。
- 2、存取及處理個人資料之資訊設備與會員資訊管理系統，應定期進行維護及安全管理。委外建置之系統設備於維護、更新或異動時，應注意個人資料之備份、存取權限及相關安全措施，以維護資料安全。
- 3、存放個人資料之電腦設備、其他媒介物如須報廢汰換或轉作其他用途時，本會理事長或經指定之管理人員應檢視該設備所儲存之個人資料是否確實刪除。

(二) 資料安全管理

1、電腦存取個人資料之管控：

- (1) 個人資料檔案儲存於學會個人電腦時，應在該電腦設置登入密碼、資料保護密碼及相關安全措施。
- (2) 本會會務工作人員如因職務內容而須使用任一個人資料時，須於個人資料管理系統輸入個人識別帳號與密碼，並只得應用資料於相關職務內容。其中個人識別帳號及密碼並應保密，不得洩漏或與他人共用。
- (3) 個人資料檔案使用完畢應立即登出相關系統或關閉資料畫面，不得任意留置於可供他人閱覽之資訊設備介面。
- (4) 定期進行電腦系統防毒、掃毒之必要措施。
- (5) 重要個人資料之存取權限，應由指定管理人員核可後授予，並採取適當之密碼及存取控制措施。

2、紙本資料之保管：

- (1) 對於個人資料表、名冊等記載個人資料之紙本資料，應存放於公文櫃內並上鎖，會務工作人員非經代表人或經指定之管理人員同意不得任意複製或影印。
- (2) 對於記載個人資料之紙本資料丟棄時，應先以碎紙設備進行處理。

3、本會使用資通訊系統蒐集、處理或利用會員（會員代表）個人資料採取下列資訊安全措施：

- (1) 使用者身分確認及保護機制。
- (2) 個人資料顯示之隱碼機制。
- (3) 網際網路傳輸之安全加密機制。
- (4) 個人資料檔案與資料庫之存取控制及保護監控措施。
- (5) 防止外部網路入侵對策。

(6) 非法或異常使用行為之監控及因應機制

(三) 人員安全管理

- 1、本會依會務需求，得適度設定所屬會務工作人員（例如主管、非主管人員）不同之權限，以控管其得接觸、使用或處理之個人資料情形。
- 2、本會會務工作人員每 3 個月應變更識別密碼 1 次，並於變更識別密碼後始可繼續使用電腦。
- 3、會務工作人員離職，將立即取消其使用者帳號及密碼。其所持有之個人資料應辦理交接，不得在外繼續使用，並簽訂保密切結書（如在任職時之相關勞務契約已有所約定時，亦屬之）。
- 4、本會會務工作人員應妥善保管個人資料之儲存媒介物，執行會務時依個人資料保護法規定蒐集、處理及利用個人資料。
- 5、本會與會務工作人員所簽訂之相關勞務契約或承攬契約均列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務（含契約終止後）。

九、認知宣導及教育訓練

- (一) 本會每年進行個人資料保護法基礎認知宣導及教育訓練至少乙次，使會務工作人員知悉應遵守之規定。前述認知宣導及教育訓練應留存紀錄（例如：簽名冊等文件）。
- (二) 對於新進人員應特別給予指導，務使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

十、個人資料安全維護稽核機制

- (一) 本會定期（每年至少 1 次）辦理個人資料檔案安全維護稽核，檢查本會是否落實本計畫及處理方法規範事項，針對檢查結果不符合事項及潛在不符合之風險，應規劃改善措施，並確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：
 - 1、確認不符合事項之內容及發生原因。
 - 2、針對稽核結果提出改善及預防措施方案。
 - 3、紀錄及追蹤檢查情形及結果。
- (二) 前項檢查情形及結果應載入稽核報告中，由代表人簽名確認。

十一、使用紀錄、軌跡資料及證據保存

- (一) 本會建置個人資料之電腦，其使用、查詢個人資料之紀錄檔，應每年定期備份加密，並將該紀錄檔之儲存媒介物保存於理事長辦公室之公文櫃以供檢查。
- (二) 個人資料使用紀錄以紙本登記者，應存放於理事長辦公室之公文櫃內並上鎖，或使用電子數位化方式取代，處理全部或部分資料及證據保存，非經本會代表人或經指定之管理人員同意，不得任意取出。

十二、個人資料安全維護之整體持續改善

- (一) 本會應隨時參酌會務及本計畫及處理方法之執行狀況、社會輿情、技術發展及相關法規訂修等因素，檢討所定本計畫及處理方法，必要時予以修正；修

正時，應於 15日內將修正後之本計畫及處理方法報請主管機關備查。

(二) 針對個資安全稽核結果不合法令之虞者，規劃改善與預防措施。

十三、會務終止後之個人資料處理方法

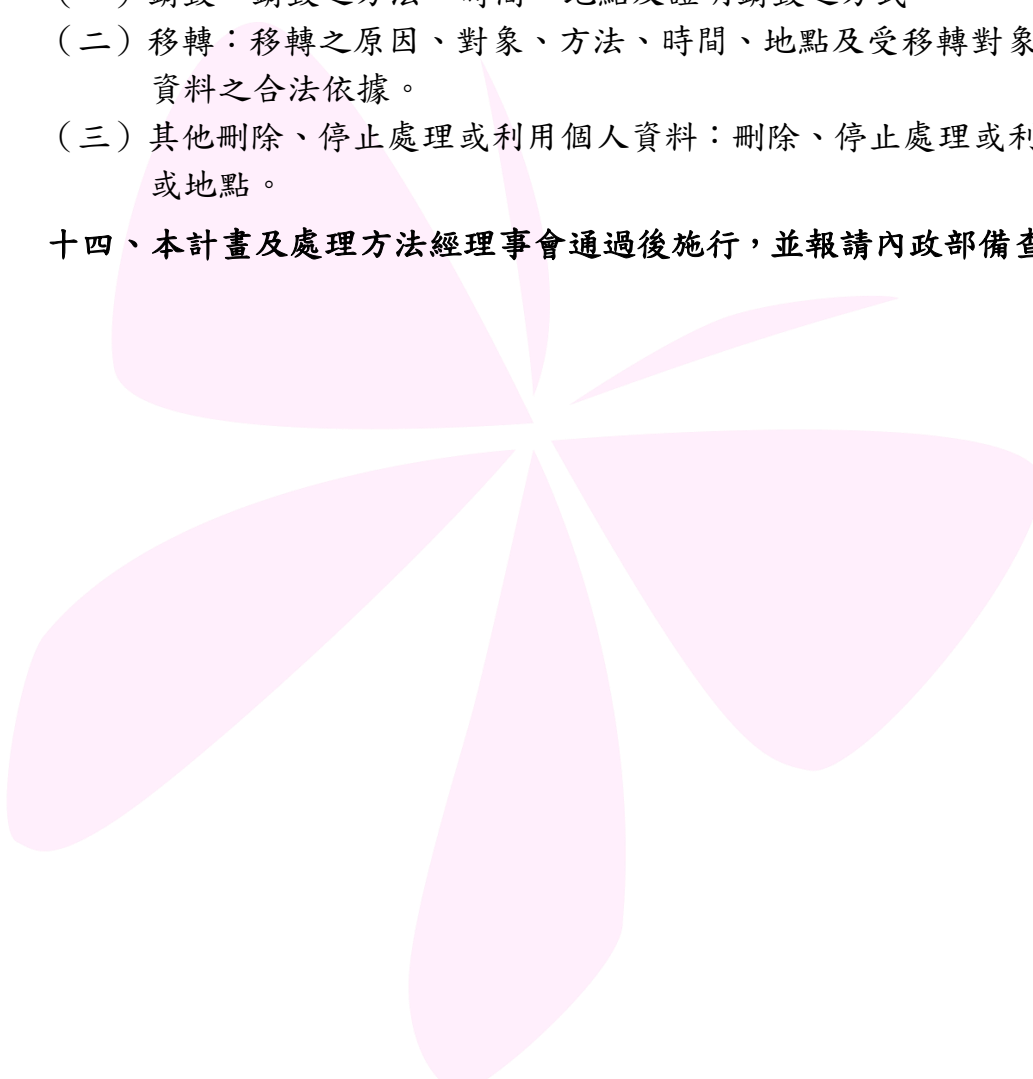
本會會務終止後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，並留存相關紀錄，其保存期限至少五年：

(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。

十四、本計畫及處理方法經理事會通過後施行，並報請內政部備查，變更時亦同。



TAOHN

附件

個人資料事故通報紀錄表		
非公務機關名稱 _____ 通報機關 _____	通報時間： 年 月 日 時 分	
	通報人： 簽名（蓋章）	
	職稱：	
	電話：	
	Email：	
	地址：	
發生時間		
發生種類	☐ 竊取 ☐ 竄改 ☐ 毀損	個人資料侵害之總筆數（大約） _____
	☐ 滅失 ☐ 洩漏 ☐ 其他侵害情形	☐ 一般個人資料 _____ 筆 ☐ 特種個人資料 _____ 筆
發生原因及摘要		
損害狀況		
個人資料侵害可能結果		
擬採取之因應措施		
擬通知當事人之時間及方式		
是否於發現個人資料外洩後七十二小時內通報	☐ 是 ☐ 否，理由：	

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。