高敏感(風險)個人資料

資訊隱私管理指引

機 密 等 級：內部使用
版　　次：V 1.0
制（修）訂日期：115 年 7 月 8 日

制 修 訂 紀 錄

版次	制（修）訂日期	修訂者	制（修）訂內容摘要
V0.1	115.4.1	衛生福利部資訊處	初稿起草
V0.9	115.4.15	衛生福利部資訊處	內部審閱修訂
V1.0	115.7.8	衛生福利部資訊處	正式發布

目錄

壹、目的

為避免業務授權人員違規查詢高敏感(風險)個人資料，本指引提供各單位從識別高敏感(風險)個資、建立預防措施、事中即時告警、事後稽核的完整操作框架。

貳、作業說明

一、 識別高敏感(風險)個人資料

（一）包含《個人資料保護法》所定義之特種個人資料、弱勢成人或未成年人之個人資料，以及其他具敏感性之資料。

（二）依照本部【CC-PI-02-003 個人資料檔案盤點暨風險評鑑管理程序】所定之風險評鑑作業，經評估認定具有高度風險之資料。

二、 事前預防措施

（一）資訊系統應依其防護需求等級，符合《資通安全責任等級分級辦法》附表十所定防護基準之存取控制、識別與鑑別等控制措施要求。

（二）另應依本部【CC-IS-02-016 資訊存取安全管理程序】辦理系統帳號及權限管理、職務權責區隔、存取權限管理及帳號全面清查等措施。

（三）申請介接、使用高敏感(風險)個人資料時，申請機關應訂管理規定，並敘明下列事項：

1. 法律依據、或重大政策依據及計畫。
2. 使用資料之目的、適用機關、業務範圍及資料安全管制作業。
3. 處理資料之保密措施。
4. 使用者查詢資料之具體授權及作業程序。
5. 指定專責人員辦理安全維護事項。
6. 自提供機關取得之資料使用期限、銷毀程序及銷毀

期限。

7. 定期督考查核及配合提供機關實施稽核作業之具體程序，每半年至少辦理一次自我稽核。
8. 資料使用期間每月應抽查使用紀錄，其抽查比率不得低於查詢件數之百分之七十。
9. 對於取得資料之處理及利用，違反個人資料保護法規定致當事人權益受損時應負之責任。
10. 使用者違反規定時應負之責任。

三、 事中告警

（一）具高敏感(風險)個人資料之系統，應定義使用者異常行為。參考範例如下：

行為類型	說明
非管轄案件查詢	查閱非本人負責個案之資料
大量批次查詢	一小時內查詢超過 10 筆非負責個案
特定特徵過濾搜尋	以年齡、性別等條件大範圍過濾瀏覽
非辦公時間存取	深夜、假日存取高敏感(風險)資料
反覆查詢同一對象	30 天內多次查閱同一當事人
串接查詢	同一人在系統交叉比對個案
異常 IP 或地理位置	從不常見網路位置登入
規避 MFA 驗證	試圖繞過多重驗證

（二）使用者觸發異常行為時，系統應自動採取合規提醒、通知系統管理員、停用帳號等必要應變措施。

四、 事後稽核

（一）系統應依《資通安全責任等級分級辦法》附表十所定

防護基準，完整記錄系統事件日誌並妥善保存，保存期限應符合相關法規要求。

（二）所有高敏感(風險)個資之存取操作均應留存日誌，日誌欄位至少包含

1. 可識別操作者資訊：帳號、姓名、職稱
2. 存取資訊：時間、IP 位址、登入地點
3. 操作類型：查詢、修改、列印、匯出、刪除
4. 查詢條件、查詢事由。

（三）應定期辦理稽核作業，並留存紀錄備查，應涵蓋的項目建議如下：

1. 存取權限

（1）確認帳號清單是否與現職人員一致，無離職或調職人員殘留帳號。

（2）確認各帳號權限是否符合最小權限原則，無過度授權情形；確認高權限帳號（如系統管理員）是否有額外控管措施。

（3）確認臨時或跨區授權是否已於時效後自動撤銷。

2. 日誌完整性

（1）確認日誌是否涵蓋所有必要欄位（操作者、時間、IP、操作類型、查詢事由等)。

（2）確認日誌是否連續完整，有無異常中斷或遺漏。

（3）確認日誌儲存於獨立伺服器且具不可竄改保護。

（4）確認日誌保存期限是否符合法規要求。

3. 異常行為處理

（1）確認系統自動標記之異常行為是否已完成後續處理與回應。

（2）核實非辦公時間存取、跨區查詢、大量批次查詢

等高風險行為之業務必要性。

4. 查詢紀錄稽核

(1) 隨機抽查查詢紀錄，由主管核實必要性並簽署確認，針對敏感操作（匯出、列印、刪除等）應提高抽樣比例。

(2) 高權限帳號之操作紀錄應逐筆審查，不得以抽樣替代。

參、重要資訊系統預防濫權安全檢查表

系統名稱：_____評估日期：_____

項次	查檢項目	說明	符合	不符合	不適用	改善措施/ 預計完成日期
一、事前預防						
1	職責分離（SoD）	系統是否區分使用者、管理者等角色 職務高低不等同權限高低				
2	最小權限原則	使用者是否僅能存取其業務轄區或負責個案之資料，無法瀏覽非指派範圍 常見錯誤設計：以高職務者有較大的資料範圍查詢權限				
3	記錄查詢事由	系統是否於查詢前強制要求填寫查詢事由及案號				
4	多因素驗證	登入或執行高敏操作時是否執行二次驗證				
5	帳號定期清查	是否至少每半年執行一次全體帳號（含管理者及使用者）之權限清查與複審				
6	臨時權限管理	臨時權限是否需經申請核准程序，並於時效後自動撤銷				
7	離職／調職即時處理	人員離職或職務異動時，是否立即停用帳號				
8	敏感欄位遮罩	一般列表中，身分證號、電話、住址等敏感欄位是否預設部分遮蔽				
9	動態浮水印	於高風險系統介面是否顯示操作者帳號、IP 及時間戳記之動態浮水印，以防截圖				

		或拍照外流				
10	資料下載	批次(大量)下載或列印，事前審核程序完備，且下載檔案有適當加密及浮水印				
二、事中告警						
1	異常行為監控	系統定義異常行為，並設定對應防禦措施				
三、事後稽核						
1	完整日誌留存	所有高風險個人資料之存取操作是否完整留存日誌，並涵蓋操作者帳號、姓名、職稱、存取時間、IP 位址、登入地點、查詢對象識別碼、操作類型及查詢事由等欄位？				
2	不可竄改日誌	稽核日誌是否定期備份至獨立伺服器，且無法自行修改或刪除				
3	定期隨機抽樣稽核	是否每週隨機抽取查詢紀錄，要求主管核實操作必要性並簽署確認				
4	稽核紀錄備查	審查完成之稽核紀錄是否定期提交系統管理業管單位留存備查				

肆、參考文件

一、CC-PI-02-001 個人資料檔案蒐集處理與利用管理程序

二、CC-PI-02-003 個人資料檔案盤點暨風險評鑑管理程序

三、CC-IS-02-016 資訊存取安全管理程序