健曄醫康科技股份有限公司個人資料安全維護計畫

115 年 1 月 2 日 1 版

健曄醫康科技股份有限公司（下稱本公司）依據個人資料保護法、數位經濟相關產業個人資料檔案安全維護管理辦法等相關規範，訂定以下個人資料安全維護計畫(下稱本計畫)，作為本公司個人資料保護管理機制之最高指導文件。

一、配置管理人員及相當資源

（一）配置管理人員（成立個資小組）

個資保護總負責人: 技術總監 陳家興

個資管理專職人員: 辦公室主任 楊景婷

（二）配置相當資源

預算：115 年新臺幣壹佰萬元。

二、個人資料保護管理政策

本公司對內公開周知以下個人資料保護管理政策：

1.遵守我國個人資料保護相關法令規定。

2. 依照本計畫所列個人資料蒐集、處理及利用之內部管理程序內容，於特定目的範圍內，蒐集、處理或利用個人資料。

3. 依照本計畫所列資料安全管理內容，以可期待之合理安全水準技術保護其所蒐集、處理或利用之個人資料檔案。

4. 本公司之個資聯絡窗口：

(1) 個資當事人行使其個資相關權利或提出相關申訴與諮詢聯絡窗口：辦公室主任: 楊景婷，連絡電話: 02-6636-7777

(2) 事故通報個資聯絡窗口：辦公室主任: 楊景婷，連絡電話: 02-6636-7777

(3) 緊急應變程序依照本計畫第五點所列之內容進行。

(4) 監督委外廠商依照本計畫第十三點所列內容進行。

(5) 持續維運安全維護計畫之義務，依照本計畫第十五點所列之內容進行以確保個人資料檔案之安全。

三、清查（盤點）及界定個人資料之範圍

（一）清查（盤點）及界定頻率：每年進行清查盤點及界定一次。

（二）蒐集、處理或利用個資之屬性

1. 所屬人員（含員工、業務、兼職、派遣、顧問、股東等人員）
2. 消費者（含代管或暫存）
3. 廠商客戶聯繫窗口
4. 供應商、承包商聯繫窗口

（三）個資盤點方式

本公司採用系統化與文件化並行的方式進行個人資料盤點。首先以資訊系統為核心，盤查公司各項業務系統與資料庫中所涉及的個人資料類型，釐清資料的蒐集來源、使用目的、儲存位置與使用部門；同時透過部門盤點表，由各業務單位填報在業務流程或文件表單中所蒐集與使用的個人資料。
在完成資料來源盤查後，本公司進一步整理個人資料於蒐集、傳輸、處理、儲存及刪除等各階段的資料流向，建立完整的個資清冊與資料流程紀錄，以掌握個資生命週期與管理責任。透過上述盤點機制，可確保公司全面掌握個人資料的處理情形，作為後續個資保護措施、權限管理及資安風險評估的重要依據。

四、個人資料之風險評估及管理機制

（一）評估頻率：每年進行評估一次。

（二）方法說明

本公司為確保個人資料之安全與合規使用，建立完善之個人資料風險評估與管理機制。首先透過個資盤點與資料流向分析，掌握公司於蒐集、處理、利用、傳輸及保存過程中涉及之個人資料類型、來源與使用目的，並依據資料敏感度及業務重要性進行風險分級管理。

在風險評估方面,本公司定期檢視個人資料可能面臨之未經授權存取、資料外洩、誤用或系統漏洞等風險，並透過權限控管、資料備份、系統監控及存取紀錄管理等技術與管理措施降低風險發生之可能性。同時針對涉及個人資料之資訊系統與作業流程，持續進行安全檢核與改善。

此外，本公司建立個資事件通報與應變機制，若發生疑似個資外洩或資安事件，將立即啟動通報、調查與處置流程，以降低影響範圍並防止事件擴大。透過定期檢討與持續改善，本公司持續強化個人資料保護措施，確保個人資料之安全與完整性。

五、事故之預防、通報及應變機制

（一）訂定事故應變流程計畫

1. 發生個資事故時，通報事故通報個資聯絡窗口、並由個資小組啟動應變程序，各項應變程序皆完成後始可結案。

    - 事故通報：72 小時內通報主管機關數位發展部並配合調查。
    - 通知當事人：初步查明後立即以適當方式通知當事人，使當事人知悉個資事故及已採取之因應措施。
    - 通知客戶：立即通知客戶並配合協助通知當事人，使當事人知悉個資事故及已採取之因應措施。
    - 事故排除及追蹤：立即採取事故排除措施、改善措施，以及後續追蹤。

2. 事故預防、通報及應變機制之演練。

（二）事故通報

1. 通報時點：知悉發生事故 72 小時內。
2. 通報條件：遇有個人資料安全事故，將危及其正常營運或大量當事人權益。
3. 通報對象：數位發展部。電話：02-23808390；信箱：www-mailbox.adi.gov.tw

4. 通報內容：事件發生種類、外洩大略筆數、發生原因及事件摘要、採取的因應措施、通知當事人的時間和方法。（使用數位經濟相關產業個人資料檔案安全維護管理辦法附表二）
https://law.moda.gov.tw/Download.ashx?FileID=751

附表二　業者個人資料外洩通報表

個人資料侵害事故通報與紀錄表		
業者名稱 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：	
事件發生時間		
事件發生種類	□竊取 □洩漏 □竄改 □毀損 □滅失 □其他侵害事故	個人資料侵害之總筆數(大約) _____筆
		□一般個人資料_____筆 □特種個人資料_____筆
發生原因及事件摘要		
損害狀況		
個人資料外洩可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於知悉個人資料外洩後72小時通報	□是　□否，理由：	

（三）通知當事人

1. 通知時點：自知悉時起即初步查明，並立即以適當方式通知當事人。
2. 通知條件：遇有個資被竊取、洩漏（個資外洩）或竄改、損毀、滅失之事故。
3. 通知內容：使當事人知悉個資遭外洩或竊取、已採取哪些應對及修補措施。查明事故後亦通知當事人事故之發生與處理情形，及後續供當事人查詢之電話專線或其他適當管道。
4. 通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。

（四）通知客戶：

1. 通知時點：自知悉時起即應盡速通知。
2. 通知條件：遇有個資被竊取、洩漏（個資外洩）或竄改、損毀、滅失之事故。
3. 通知內容：使當事人知悉個資遭外洩或竊取、已採取哪些應對及修補措施。
4. 通知方式：以簡訊、電子郵件等其他足以使當事人知悉或可得知悉之方式。

（五）事故排除及追蹤：

本公司將採取以下事故排除措施、改善措施及後續追蹤：

1. 事故發生後之應變措施:

   當發生疑似個人資料外洩或資安事件時，本公司將立即啟動應變機制，先行隔離受影響之系統或設備，停止相關服務或暫停伺服器運作，以避免損害持續擴大。同時進行惡意程式掃描與清除、關閉異常帳號或連線，並採取必要之技術措施降低對當事人可能造成之損害，確保系統與資料之安全。

2. 調查事件成因及入侵方式:

   事件發生後，本公司將進行事件調查與分析，包括調閱系統存取紀錄（Log）、檢視系統設定與權限管理情形、檢查可能存在之系統漏洞或弱點，並分析是否存在未授權存取或其他可能導致事件發生之原因，以釐清事故發生之成因與影響範圍。

3. 矯正與預防措施機制:

   依據事件調查結果，本公司將研擬並實施必要之矯正與預防措施，例如強化資訊安全防護措施、修補系統漏洞、調整帳號與權限管理機

制、改善個人資料蒐集與處理流程，並視需要重新檢視與合作廠商或客戶之資安責任與管理機制，以防止類似事件再次發生。

4. 後續追蹤與持續改善:

本公司將針對事件處理結果進行後續追蹤與檢討，確認改善措施確實落實並持續監控系統運作狀況，並將相關經驗納入公司資訊安全管理制度中，作為未來風險評估與防護機制強化之參考依據。

（六）事故預防、通報及應變機制之演練

1. 定期檢視頻率：每一年定期演練一次。
2. 演練內容：測試異常存取資料監控機制、異常存取資料行為事故通報及應變機制。

六、個人資料蒐集、處理及利用之內部管理程序

（一）個資蒐集、處理或利用符合法定要件：

確認個資同意書、隱私權政策等相關約定內容，以及實際蒐集、處理或利用個資檔案時，是否符合以下法定要件：

1. 特定目的

(1) 利用個資時符合蒐集時之利用目的。

(2) 目的外利用個資，符合個資法第 20 條下列事由：

- 法律明文規定。
- 為增進公共利益所必要，公共利益。
- 為免除當事人之生命、身體、自由或財產上之危險。
- 為防止他人權益之重大危害。
- 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 經當事人同意。(應先告知個資法第 8 條所定應告知事項)

- 有利於當事人權益。
- 特種個資不得目的外利用。

2. 法律依據

(1) 特種個資，符合個資法第 6 條所訂之法律依據

- 法律明文規定。
- 業者履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 當事人自行公開或其他已合法公開之個人資料。
- 學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 經當事人書面同意。(應先告知個資法第 8 條所定應告知事項)。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

(2) 一般個資，符合個資法第 19 條之法律依據

- 法律明文規定。
- 與當事人有契約或類似契約之關係，且已採取適當之安全措施。
- 當事人自行公開或其他已合法公開之個人資料。
- 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 經當事人同意。(應先告知個資法第 8 條所定應告知事項)
- 為增進公共利益所必要。
- 個資取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。
- 對當事人權益無侵害。

3. 告知當事人

(1) 告知個資當事人，符合個資法第 8、9 條之規定

A. 直接向當事人蒐集個資時，明確告知當事人下列事項：

- 業者名稱。
- 蒐集之目的。
- 個人資料之類別。
- 個人資料利用之期間、地區、對象及方式。
- 當事人依第三條規定得行使之權利及方式。
- 當事人得自由選擇提供個資時，不提供將對其權益之影響。

B. 蒐集非由當事人提供之個資時，明確告知當事人下列事項：

- 公務機關或非公務機關名稱。
- 蒐集之目的。
- 個人資料之類別。
- 個人資料利用之期間、地區、對象及方式。
- 當事人依第三條規定得行使之權利及方式。

(2) 符合免為告知之情形

A. 直接向當事人蒐集個資時符合免為告知之情形

- 依法律規定得免告知。
- 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
- 告知將妨害公務機關執行法定職務。
- 告知將妨害公共利益。
- 當事人明知應告知之內容。
- 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

B. 蒐集非由當事人提供之個資時符合免為告知之情形

- 依法律規定得免告知。
- 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

- 告知將妨害公務機關執行法定職務。
- 告知將妨害公共利益。
- 當事人明知應告知之內容。
- 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。
- 當事人自行公開或其他已合法公開之個人資料。
- 不能向當事人或其法定代理人為告知。
- 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。
- 大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

4. 最小化原則（比例原則）

蒐集個資時不蒐集與利用目的無關的個資。

5. 國際／境外傳輸之限制、告知

本公司未進行個人資料國際傳輸。

6. 定期檢視個人資料蒐集之特定目的是否已消失或期限是否已屆滿

（1）每一年定期利用個資盤點表檢視個人資料蒐集之特定目的是否已消失，或期限是否已屆滿。

（2）個人資料之特定目的消失或期限屆滿時，依個資法第 11 條第 3 項規定處理：

- 主動刪除、停止處理及停止利用該個人資料。
- 因法規規定、執行職（業）務所必須，或經當事人書面同意者，可不刪除、停止處理或利用。但應於個資盤點表中寫明特定目的消失或期限屆滿時，不刪除、停止處理或停止利用之事由。

7. 個資是否委外處理或傳輸至第三方

(1) 傳輸第三方對象：客戶授權並簽訂保密協議之第三方對象。

（二）受理當事人請求權利之程序

1. 受理內容

（1）拒絕行銷之處理程序

（2）受理當事人行使個資法第 3 條權利之程序

（3）受理個資更正之程序

2. 拒絕行銷受理方式：

（1）當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

（2）首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

（3）提供當事人免費、快速、容易表達之簡便方式。

3. 當事人行使個資法第 3 條權利受理方式：

(1) 告知當事人得依個資法第 3 條規定得行使之權利及方式

(2) 至少與蒐集當事人個資相同之方式、管道、難易度相同。

(3) 受理後處理方式包含：

- 確認當事人或其代理人之身分。
- 檢視是否符合個資法第 10 條但書、第 11 條第 2 項但書及第 11 條第 3 項但書所定得拒絕其請求之事由。
- 拒絕當事人行使權利者，附理由通知當事人。
- 當事人請求為准駁決定及延長決定期間之程序，並應確保符合個資法第 13 條之規定。
- 當事人請求更正或補充其個人資料者，其應釋明之事項。
- 當事人查詢、請求閱覽或製給複製本之請求酌收必要成本費用者，應明定其收費標準。

4. 個資更正受理方式：

（1）維護個人資料之正確，並主動或依當事人之請求更正或補充之。

（2）提供當事人免費、快速、容易表達之簡便方式請求更正或補充之。

(3) 個資正確性有爭議者，應主動或依當事人之請求停止處理或利用。

(4) 因可歸責於本公司之事由，未為更正或補充之個資，應於更正或補充後，通知曾提供利用之對象。

七、資料安全管理

（一）本公司提供之基層醫療院所資訊服務系統服務，自行、或協助客戶蒐集、處理或利用個人資料時，提供 SaaS 服務（存於 GCP 雲端伺服器），採取以下資料安全管理措施：

1. 加密：個人資料有加密之必要時，於透過 API 傳輸資料時採取 AES-256 以上之加密演算法等加密措施。且解密金鑰與加密資料應存放於不同位置。

2. 備份：備份資料採取備份資料採取 321 備份原則、加密儲存與自動備份機制 之保護措施。且備份區儲存位置應與正式區及測試區進行隔離。

3. 傳輸安全：透過 API 進行資料傳輸時，採取 TLS 1.2 以上傳輸安全協定 之安全措施，並通過 弱點掃描與安全檢測 相關檢測。

4. 外部網路入侵對策：

(1) 建置防火牆：管理系統伺服器及 OA 區網路防火牆只開放必要的通訊埠對外連線，並每半年定期更新一次。

(2) 其他入侵偵測設備：安裝中華電信 Hinet 資安艦隊進行資安保護。

5. 異常行為之監控及因應演練：

(1) 異常行為之監控

伺服器內設置異常登入行為監控設備與記錄檔(log)儲存與備份機制。

(2) 異常行為因應演練：每一年定期演練異常存取資料行為因應機制。

6. 檢測系統漏洞及修補：

(1) 開發之資訊服務系統產品提供給客戶前，應至少進行 1 次進行源碼掃描檢測系統漏洞，並修補漏洞至無中風險及高風險漏洞。

(2) 若與客戶訂有維護契約時,每一年定期一次透過系統網站弱點掃描、主機弱點掃描,檢測伺服器及相關系統漏洞，並修補漏洞至無中風險及高風險漏洞。

7. 防毒軟體及惡意程式檢測：

(1) 設備及系統隨時更新及執行防毒軟體。

(2) 每半年定期執行惡意程式檢測一次。

8. 密碼及認證機制：

(1) 密碼管理機制:

- 為確保資訊系統帳號安全，本公司訂定密碼管理規範如下：密碼長度不得少於 8 碼，並應包含 英文字母、數字及特殊符號之組合。
- 使用者不得使用與帳號相同或過於簡單之密碼（如 123456、password 等）
- 系統應定期要求使用者 更換密碼（至少每 90 日更換一次）。
- 密碼不得與他人共用，並應避免記錄於公開或不安全之場所。
- 系統應設定 登入錯誤次數限制，當連續登入失敗達一定次數時，系統將暫時鎖定帳號，以防止暴力破解。
- 當使用者離職或職務調整時，應立即停用或調整相關系統帳號權限。

(2) 其他認證機制：雙因子認證（2FA）：

為提升帳號安全性，本公司於重要系統(如雲端服務、管理後台等)導入 雙因子認證機制（Two-Factor Authentication, 2FA），於使用者登入時除輸入帳號密碼外，需再透過以下方式之一進行驗證：

- 手機驗證碼（OTP）
- 身分驗證應用程式（Authenticator）
- 其他安全驗證方式

透過多重驗證機制，以降低帳號遭未授權存取之風險。

9. 避免利用真實個資測試：

(1) 處理個資之資通系統進行測試時避免使用真實個資。

(2) 使用真實個資者，應訂定使用規範。

10. 資訊系統變更：處理個資之資通系統有變更時，應確保其安全性未降低。

11. 定期檢查：每一年一次定期檢視處理個資之資通系統，檢查其使用狀況及存取個資之情形。

（二）本公司產品開發政策

本公司提供之基層院所醫療資訊管理系統服務系統服務，採取以下產品開發政策：

1. 隱私保護設計原則（Privacy by Design）
   在系統設計與開發初期即納入個人資料保護與資訊安全考量，於需求分析、系統設計、開發與測試等階段均評估個資保護需求，以降低個資外洩與濫用之風險。
2. 最小必要原則:
   系統僅蒐集與處理提供醫療資訊服務所必要之個人資料，避免過度蒐集，並依據業務需求限制資料存取範圍。
3. 權限控管與身分驗證:
   系統設計採分級權限管理機制，依使用者角色（如醫師、藥師、行政人員等）設定不同存取權限，並透過帳號密碼管理及相關身分驗證機制，確保資料僅供授權人員使用。
4. 資料安全保護措施:
   系統於資料傳輸與儲存過程中採取適當之安全措施，例如加密傳輸、存取紀錄（Log）管理、資料備份與系統監控等，以確保個人資料之機密性與完整性。
5. 系統維護與安全更新
   本公司定期進行系統安全檢查與版本更新，修補已知漏洞並強化資安防護機制，以確保系統持續符合相關法規與資訊安全要求。
6. 測試與資料保護
   在系統測試或開發環境中，避免使用真實個人資料，必要時將資料進行去識別化或匿名化處理，以降低個資外洩風險。

（三）本公司之公司 OA 區電腦、共用區等設備，採取以下資料安全管理措

施：

1. 加密：儲存於公司共用區設備之資料採取 AES256 之加密措施。且解密金鑰與加密資料應存放於不同位置。

2. 備份：備份資料採取 321 備份原則及加密自動備份機制之保護措施。且備份區儲存位置應與正式區及測試區進行隔離。

3. 傳輸安全：資料透過 VPN 或 HTTPS 傳輸時，採取 TLS 1.2 以上傳輸安全協定 之安全措施。

4. 外部網路入侵對策：

(1) 建置防火牆：管理系統伺服器及 OA 區網路防火牆只開放必要的通訊埠對外連線，並每半年定期更新一次。

(2) 建置應用程式防火牆：網站安裝應用程式防火牆監測、過濾、阻斷可疑的流量，並每半年定期更新一次。

(3) 電子郵件過濾機制：員工電子郵件系統採取過濾系統，每半年定期更新一次。

(4) 端點防護：OA 區電腦、共用區設備採取端點防護，每半年定期更新一次。

(5) 其他入侵偵測設備：安裝中華電信 Hinet 資安艦隊監控系統。

5. 異常存取資料行為之監控及因應演練：

(1) 異常行為之監控

伺服器內設置異常登入行為監控設備、系統內設置異常存取資料行為監控設備。

(2) 異常行為因應演練：每一年定期演練異常存取資料行為因應機制。

6. 檢測伺服器及相關系統漏洞及修補：每一年定期一次透過網站弱點掃描及主機弱點掃描檢測伺服器及相關系統漏洞，並修補漏洞至無中風險及高風險漏洞。

7. 防毒軟體及惡意程式檢測：

(1) 設備及系統隨時更新及執行防毒軟體。

(2) 每半年定期執行惡意程式檢測一次。

8. 密碼及認證機制：

（1）密碼

（2）其他認證機制：雙因子認證（2FA）

9. 避免利用真實個資測試：

(1) 處理個資之資通系統進行測試時避免使用真實個資。

(2) 使用真實個資者，應訂定使用規範。

10. 資訊系統變更：處理個資之資通系統有變更時，應確保其安全性未降低。

11. 定期檢查：每一年一次定期檢視處理個資之資通系統，檢查其使用狀況及存取個資之情形。

12. 個資隱碼：針對系統或伺服器之資料庫儲存資料、API 傳輸資料及前端系統查詢畫面之個資使用情境，採行 資料庫加密、TLS 傳輸加密及前端畫面部分遮罩顯示之隱碼機制。

八、人員安全管理

1. 保密義務約定：與所屬人員約定保密義務，約定方式：簽署保密協議書（NDA)。

2. 識別人員：識別業務內容涉及個資蒐集、處理或利用之人員。識別方式：依專案分工及系統帳號權限管理識別。

3. 人員存取權限之控制：依業務特性、內容及需求，設定所屬人員接觸個資之權限，並定期檢視適當性及必要性。

（1）實體空間人員進出管制措施：錄影與門禁管理

(2)系統共用文件區存取管制措施：依專案及部門設定資料夾存取權限

4. 人員離職時之資料返還程序：要求離職人員返還所有設備與資料載體

並刪除帳號權限

九、設備安全管理

1. 儲存媒介物：依存有個資之儲存媒介物(紙本、光碟片、電腦、自動化機器設備及其他媒介物等）之特性及使用方式，訂有以下管理規範：

(1) 設備維護安全管理措施：端點防護與定期系統更新

(2) 儲放環境安全管理措施：共用區資料夾權限管理及門禁管制

2. 人員保管規範：存有個人資料之設備或儲存媒介物由指定人員負責保管與使用，並依權限管理制度進行控管。未經授權人員不得存取或複製相關資料，亦不得將含有個資之設備或資料媒介攜出公司或提供他人使用。如因業務需要攜出設備，須經主管同意並採取必要之安全保護措施。

3. 人員進出管制規範：存放個人資料之辦公區域及設備環境採取門禁管理機制，僅限授權人員進出。訪客或非相關人員進入辦公區域時，須經公司人員陪同，並避免接觸或存取含有個資之設備、文件或儲存媒介。

4. 過期資料及設備處理措施：當設備、儲存媒介或資料已達保存期限或不再使用時，應依公司資料銷毀與設備處理程序辦理。對於紙本資料以碎紙機或委託合格銷毀廠商處理；電子資料則透過安全刪除、資料覆寫或儲存媒體銷毀等方式進行處理，以確保資料無法復原。

十、個資保護認知宣導及教育訓練

1. 定期舉辦全體員工一般訓練，每一年至少一次。

(1) 個人資料保護相關法令之規定

(2) 所屬人員之責任範圍

(3) 本計畫各項管理程序、機制及措施之要求

(4) 個資保護及資安意識

(5) 社交工程演練或辨識社交工程之教學

2. 定期舉辦個資小組人員（代表人、負責人及管理人員）特殊訓練，每一年至少一次。

3. 資訊人員定期參加特殊訓練，每一年至少一次。

4. 留存教育訓練實施紀錄，包括

- 簽到簽退
- 製作會議紀錄
- 課後評量機制

十一、使用紀錄、軌跡資料及證據保存

（一）個資之蒐集、處理或利用紀錄

1. 公司 OA 區電腦、共用區等設備

(1) 保存方法：電子紀錄保存於公司 NAS 及 GCP 雲端

(2) 保存地點：公司 NAS 及 GCP 雲端儲存空間

(3) 保存期限：7 年

2. 本公司為提供客戶服務之系統

(1) 保存方法：系統 Log 電子紀錄

(2) 保存地點：GCP 雲端伺服器

(3) 保存期限：7 年

（二）自動化機器設備之軌跡資料

1. 公司 OA 區電腦、共用區等設備

(1) 保存方法：公司內部 NAS

(2) 保存地點：本公司機房

(3) 保存期限：7 年

2. 本公司為提供客戶服務之系統

(1) 保存方法：電子紀錄保存於公司 NAS 及 GCP 雲端

(2) 保存地點：公司 NAS 及 GCP 雲端儲存空間

(3) 保存期限：7 年

（三）落實執行個人資料檔案安全維護計畫之證據

1. 保存方法：公司內部 NAS

2. 保存地點：例如本公司機房、紙本紀錄存放檔案櫃或掃描檔存於共用槽

3. 保存期限：7 年

十二、個資安全稽核

本公司資料安全稽核機制如下：

（一）每一年定期檢查或稽核一次

1. 自我檢查
2. 內部稽核（由具有個資或資安稽核證照資格的同仁進行稽核）
3. 第三方外部稽核（ISO 27701），稽核範圍：全公司。

（二）檢查或稽核人員身分

1. 具個資稽核證照之人員
2. 管理人員
3. 資訊安全人員

（三）稽核結果之處理

- 作成評估報告
- 保留稽核紀錄
- 回報管理階層審查
- 立即檢討改善
- 修正本計畫

（四）檢查執行頻率

本公司為：資本額 1000 萬元以上或保有個資 5000 筆以上，每 12 個月定期執行一次安全維護措施

（五）稽核範圍

(1)本公司全辦公室範圍（含機房）

(2)本公司產品服務：基層院所醫療管理軟體

（六）稽核內容

- 配置管理之人員及相當資源
- 界定個人資料之範圍（並檢查是否定期盤點）
- 個人資料之風險評估及管理機制（並檢查是否定期評估）
- 事故之預防、通報及應變機制
- 個人資料蒐集、處理及利用之內部管理程序（並檢查是否定期評估檢視個資蒐集目的是否已消失）
- 資料安全管理措施（並檢查是否定期更新防止外部網路入侵對策、演練異常存取行為因應機制、檢測系統漏洞及修補、更新及執行防毒軟體及檢測惡意程式、檢查資通系統使用狀況及存取個資情形）
- 人員安全管理措施（並檢查是否定期檢視個資存取權限）
- 認知宣導及教育訓練（並檢查是否定期實施全體員工教育訓練、代表人及管理人員教育訓練）
- 設備安全管理
- 資料安全稽核機制（並檢查是否定期稽核或自我檢查）
- 使用紀錄、軌跡資料及證據保存
- 個人資料安全維護之整體持續改善（並檢查是否定期檢視或修正安全維護計畫）

十三、委外監督

本公司委外監督機制規劃如下：

（一）委外契約內容

本公司委託他人蒐集、處理或利用個人資料時，應對委外廠商依個人資料保護法法施行細則第 8 條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。包含：

1. 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

2. 委外廠商應採取之措施：
   - 配置管理之人員及相當資源。
   - 界定個人資料之範圍。
   - 個人資料之風險評估及管理機制。
   - 事故之預防、通報及應變機制。
   - 個人資料蒐集、處理及利用之內部管理程序。
   - 資料安全管理及人員管理。
   - 認知宣導及教育訓練。
   - 設備安全管理。
   - 資料安全稽核機制。
   - 使用紀錄、軌跡資料及證據保存。
   - 個人資料安全維護之整體持續改善。
   - 契約中其他指定事項。

3. 有複委託時，本公司之委外廠商應監督受其受託之業者。

4. 委外廠商或其受僱人違反個資法、數位經濟相關產業個人資料檔案安全維護管理辦法、其他個人資料保護法令或其法規命令時，應通知本公司並採取補救措施。

5. 委託關係終止或解除時，委外廠商應返還個人資料儲存載體，並刪除因履行委託契約而持有之個人資料。

（二）委外監督方式

為確保委外廠商在處理或接觸個人資料時符合個人資料保護相關規定，本公司建立委外監督與管理機制。於委外作業前，將審查受託廠商之資訊安全與個資保護能力，並於契約中明訂個人資料保護義務、保密責任及相關管理要求，確保受託廠商僅得於委託範圍內蒐集、處理或利用個人資料。

在委外作業期間，本公司將定期或不定期檢視受託廠商之個資保護措

施與資訊安全管理情形，必要時進行文件審查或稽核，以確認其作業符合契約約定與相關法規要求。若發現有違反規定或資安風險情形，本公司將要求其限期改善，並視情況採取必要處置措施，以確保個人資料之安全與妥善管理。

十四、業務終止後個人資料處理方法

（一）人員離職時之資料返還

1. 要求人員返還個人資料之載體，並由專責人員進行檢查。

2. 要求人員刪除因執行業務而持有之個資，並由專責人員進行檢查。

（二）因業務終止而銷毀證據保存

1. 銷毀及刪除之方法：

2. 當業務終止或個人資料已達保存期限時，本公司將依內部管理程序啟動資料銷毀作業。對於紙本資料，將以碎紙機或委託合格文件銷毀廠商進行安全銷毀；對於電子資料，則透過系統刪除、資料覆寫或儲存媒體銷毀等方式進行處理。銷毀作業完成後，相關單位須完成銷毀紀錄並回報主管單位備查，以確保個人資料確實被安全移除並避免再次被復原或利用。

3. 移轉：移轉個人資料者，應記錄其原因、對象、方法、時間、地點及受移轉對象得保有該個人資料之合法依據。

4. 其他刪除、停止處理或利用個人資料：記錄其刪除、停止處理或利用之方法、時間或地點。

5. 上述銷毀、移轉或刪除等紀錄，應保留至少 7 年。

十五、個人資料安全維護之整體持續改善

（一）安全維護計畫未落實執行時應採取矯正預防措施

1. 找出缺失之原因，以及評估是否有類似的缺失存在，或之後可能發生

缺失的項目。

2. 評估消除缺失項目所須採取的措施，並實際執行。

3. 審查所有已採取的矯正措施的有效性。

4. 將矯正措施更新於本計畫。

5. 將缺失原因、所採取之矯正措施、採取措施的過程、採取措施的結果，以文件化方式保存，做為參考依據及證據。

（二）定期檢視及修正本計畫

定期檢視頻率：每一年定期檢視及修正本計畫一次。修正內容：依據安全維護計畫矯正措施、技術發展、業務調整、法令變化等，更新內容於本計畫。