# PT-P009 患者隱私保護程序

| 文件編號 | PT-P009 | 版本 | A |
| --- | --- | --- | --- |
| 文件名稱 | 患者隱私保護程序 | 頁碼 | 1/4 |
| 制定部門 | 物理治療部 | 審核 | 管理代表 |
| 制定日期 | 2024年1月1日 | 批准 | 總院長 |
| 實施日期 | 2024年1月1日 |  |  |

## 目錄

1. 目的
2. 適用範圍
3. 權責
4. 定義
5. 程序
   * 5.1 患者隱私保護原則
   * 5.2 患者資料收集與同意
   * 5.3 患者資料管理
   * 5.4 治療過程中的隱私保護
   * 5.5 電子資料安全
   * 5.6 資料分享與傳輸
   * 5.7 患者權利保障
   * 5.8 隱私侵犯事件處理
   * 5.9 教育訓練
   * 5.10 監督與稽核
6. 記錄
7. 相關文件
8. 附件
9. 修訂紀錄

## 1. 目的

建立系統化的患者隱私保護程序，確保Ohealth物理治療系統在收集、使用、儲存和處理患者個人資料及健康資訊的過程中，符合相關法規要求，尊重並保護患者隱私權，維護患者與機構間的信任關係，提供安全且尊重個人隱私的醫療環境。

## 2. 適用範圍

本程序適用於Ohealth物理治療系統內所有涉及患者隱私與個人資料的活動，包括但不限於： - 患者資料的收集、登記與建檔 - 病歷與治療記錄的管理 - 治療過程中的隱私保護 - 個人資料的使用、儲存與傳輸 - 患者資料的銷毀 - 與患者隱私相關的溝通與投訴處理

## 3. 權責

### 3.1 院長/管理代表

* 批准患者隱私保護程序
* 提供必要資源確保隱私保護措施的實施
* 監督隱私保護程序的執行成效
* 擔任隱私保護事務的最高決策者

### 3.2 品質管理部門

* 協助制定患者隱私保護程序
* 監督程序執行情況
* 定期評估程序有效性
* 組織隱私保護相關教育訓練
* 處理隱私侵犯事件的調查與改進

### 3.3 物理治療部門主管

* 確保部門內隱私保護程序的執行
* 監督治療過程中的隱私保護措施
* 審核患者資料使用申請
* 評估並改進部門內隱私保護措施
* 參與隱私侵犯事件的調查與處理

### 3.4 病歷管理人員

* 管理患者病歷與資料的存取權限
* 監控資料使用情況
* 執行資料安全與保密措施
* 記錄資料外洩或不當使用事件
* 定期檢查資料管理系統安全性

### 3.5 資訊部門

* 確保電子病歷系統的安全性
* 實施適當的系統存取控制
* 定期評估資訊系統安全風險
* 提供系統安全性的技術支援
* 維護資料備份與災難恢復機制

### 3.6 物理治療師與工作人員

* 嚴格遵守隱私保護程序
* 妥善處理患者個人資料
* 確保治療環境的隱私性
* 報告所發現的隱私侵犯事件
* 取得患者同意後才分享其資料

## 4. 定義

### 4.1 患者隱私

指與患者相關的個人資料、健康狀況、治療過程以及其他敏感資訊，病患有權決定這些資訊的收集、使用與分享方式。

### 4.2 個人資料

能夠直接或間接識別特定個人的資訊，包括但不限於姓名、出生日期、身分證號碼、地址、電話號碼、電子郵件等。

### 4.3 健康資訊

與患者健康狀況、疾病診斷、治療計劃、治療紀錄及其他醫療相關資訊。

### 4.4 資料保密

確保患者資料僅由經授權人員在合法目的下存取、使用或披露。

### 4.5 知情同意

患者在充分了解資料收集目的、使用方式與潛在風險的情況下，自願同意機構收集、使用或分享其個人資料。

### 4.6 隱私侵犯事件

未經授權或不當收集、使用、儲存、披露或處理患者個人資料或健康資訊的行為。

### 4.7 資料處理者

代表Ohealth物理治療系統處理患者資料的內部員工或外部廠商。

### 4.8 最小必要原則

僅收集、使用或分享完成特定目的所需的最少量患者資料。

## 5. 程序

### 5.1 患者隱私保護原則

#### 5.1.1 合法性原則

* 依法收集、處理患者資料
* 確保資料處理有明確的法律依據
* 遵守相關法規與行業標準

#### 5.1.2 透明性原則

* 明確告知患者資料收集的目的與用途
* 使用易於理解的語言說明隱私政策
* 確保患者了解其權利與資料使用方式

#### 5.1.3 目的限制原則

* 僅為明確、合法、特定的目的收集資料
* 不將資料用於未告知患者的目的
* 資料使用目的變更時須重新獲取同意

#### 5.1.4 資料最小化原則

* 僅收集必要的患者資料
* 避免收集與治療無關的資訊
* 定期審查已收集資料的必要性

#### 5.1.5 正確性原則

* 確保患者資料的準確性與及時更新
* 提供患者更正不準確資料的機制
* 定期驗證資料的準確性

#### 5.1.6 儲存限制原則

* 僅在必要期間保留患者資料
* 建立資料保留與銷毀期程
* 對不再需要的資料進行安全銷毀

#### 5.1.7 完整性與保密性原則

* 實施適當的技術與組織措施保護資料
* 防止未授權存取或資料外洩
* 確保資料處理的完整性與保密性

#### 5.1.8 問責原則

* 對隱私保護措施的實施負責
* 記錄資料處理活動
* 定期評估隱私保護措施的有效性

### 5.2 患者資料收集與同意

#### 5.2.1 資料收集前的告知

收集患者資料前，應向患者告知以下資訊： - 資料收集的目的 - 收集的資料類型 - 資料的使用方式 - 資料的保存期限 - 可能的資料接收者 - 患者的權利（如存取、更正、刪除等） - 拒絕提供資料的可能後果

#### 5.2.2 知情同意的取得

* 使用專門的隱私同意書
* 確保患者充分理解同意書內容
* 提供患者足夠時間考慮
* 記錄患者的同意（書面或電子形式）
* 對於特殊類別資料（如遺傳資料）取得明確同意
* 尊重患者拒絕同意的權利

#### 5.2.3 兒童與無行為能力者的同意

* 對於未成年患者，取得其法定代理人的同意
* 對於無行為能力的成人患者，取得其監護人或法定代表的同意
* 在適當情況下，尊重兒童與無行為能力者的意願

#### 5.2.4 同意的更新與撤回

* 當資料使用目的變更時更新同意
* 提供患者撤回同意的明確機制
* 記錄同意的撤回
* 停止後續資料處理活動（法規要求的除外）

### 5.3 患者資料管理

#### 5.3.1 資料分類與標記

* 根據敏感度對患者資料進行分類
* 標記需特殊保護的資料
* 建立不同類別資料的處理指南

#### 5.3.2 資料存取控制

* 建立資料存取權限管理制度
* 實施「需要知道」的存取原則
* 定期審查並更新存取權限
* 記錄資料存取活動
* 對敏感資料實施強化的存取控制

#### 5.3.3 實體資料的保護

* 使用安全的檔案櫃儲存紙本資料
* 限制未授權人員進入資料儲存區域
* 實施清潔桌面政策
* 使用碎紙機安全銷毀不需要的文件
* 避免未經授權複製或攜出資料

#### 5.3.4 資料保留與銷毀

* 制定資料保留期限表
* 定期審查資料保留的必要性
* 建立資料銷毀程序與記錄
* 確保資料銷毀方式安全有效
* 保留資料銷毀證明

### 5.4 治療過程中的隱私保護

#### 5.4.1 治療環境的隱私性

* 使用隔間或獨立治療室
* 安裝隔音設施降低談話被聽見的風險
* 使用隔簾或屏風確保視覺隱私
* 安排適當的門診時間避免患者過度聚集
* 設計等候區域確保患者隱私

#### 5.4.2 在治療過程中的溝通

* 避免大聲討論患者的情況
* 在公共區域不使用患者全名
* 謹慎使用治療記錄與患者資訊
* 避免在其他患者面前討論敏感話題
* 提供私密空間討論敏感資訊

#### 5.4.3 治療過程的隱私保護

* 在檢查或治療前告知患者並取得同意
* 提供適當的更衣設施與遮蓋物品
* 僅暴露必要的身體部位
* 避免非必要人員在場
* 尊重患者的疑慮與要求

#### 5.4.4 學生與觀察者的管理

* 事先告知患者學生或觀察者的存在
* 獲取患者對學生或觀察者在場的同意
* 限制學生或觀察者的數量
* 確保學生或觀察者了解並遵守隱私政策
* 監督學生或觀察者的行為

### 5.5 電子資料安全

#### 5.5.1 系統安全控制

* 使用防火牆與防毒軟體保護系統
* 實施強密碼政策
* 定期更新系統與安全補丁
* 使用加密技術保護患者資料
* 建立資料備份與災難恢復機制

#### 5.5.2 使用者認證與授權

* 實施多因素認證
* 建立個人化的使用者帳號
* 定期審查使用者權限
* 及時移除離職員工的系統存取權
* 記錄系統存取與操作日誌

#### 5.5.3 行動裝置與遠端存取

* 制定行動裝置使用政策
* 對存有患者資料的行動裝置實施加密
* 啟用遠端清除功能
* 控制並監控遠端存取
* 限制敏感資料的下載

#### 5.5.4 電子通訊安全

* 使用加密傳輸患者資料
* 避免在不安全管道傳送敏感資訊
* 謹慎使用電子郵件傳輸患者資料
* 定期清理電子通訊記錄
* 提供安全的患者通訊平台

#### 5.5.5 第三方系統與服務

* 評估第三方供應商的安全措施
* 簽訂資料處理協議
* 限制第三方存取的範圍
* 監控第三方服務的使用
* 定期審查第三方安全措施

### 5.6 資料分享與傳輸

#### 5.6.1 內部資料分享

* 僅基於合法需要分享資料
* 遵循最小必要原則
* 使用安全的傳輸方式
* 記錄資料分享活動
* 確保接收者了解資料保密責任

#### 5.6.2 與外部機構的資料分享

* 僅在有明確法律依據或患者同意下分享
* 使用正式的資料傳輸協議
* 使用加密或安全傳輸管道
* 僅分享必要的資料
* 記錄所有外部分享活動

#### 5.6.3 資料傳輸安全

* 使用加密技術保護傳輸中的資料
* 採用安全的檔案傳輸協議
* 避免使用可移除媒體傳輸敏感資料
* 若使用實體媒體，確保媒體安全
* 驗證資料完整性

#### 5.6.4 資料匿名化與去識別化

* 在可能情況下使用匿名或去識別化資料
* 採用適當的去識別化技術
* 評估再識別風險
* 對去識別化資料維持適當的安全控制
* 記錄匿名化處理過程

### 5.7 患者權利保障

#### 5.7.1 患者資料存取權

* 建立患者存取其資料的程序
* 驗證請求者身份
* 在規定時間內提供資料副本
* 以易於理解的格式提供資料
* 記錄存取請求與處理過程

#### 5.7.2 更正與補充權

* 提供患者更正不準確資料的機制
* 及時處理更正請求
* 通知相關資料接收者資料已更正
* 若拒絕更正，提供理由並記錄決定
* 允許患者補充資料以完整呈現健康狀況

#### 5.7.3 刪除權（被遺忘權）

* 在適用法規允許的情況下，提供刪除選項
* 評估刪除請求的合法性
* 在合法情況下執行資料刪除
* 通知相關資料處理者刪除相關資料
* 記錄刪除活動

#### 5.7.4 限制處理權

* 允許患者在特定情況下要求限制資料處理
* 建立資料處理限制的實施機制
* 確保限制資料不被進一步處理
* 通知患者限制被解除前
* 在系統中標記受限制的資料

#### 5.7.5 資料可攜權

* 允許患者以結構化、常用且機器可讀的格式獲取資料
* 提供資料直接傳輸至其他機構的服務（若技術可行）
* 確保資料傳輸的安全性
* 驗證接收方的身份
* 記錄資料傳輸活動

#### 5.7.6 反對權

* 告知患者反對資料處理的權利
* 建立處理反對請求的程序
* 評估反對的合法性
* 若拒絕反對請求，提供清楚的理由
* 記錄反對請求與處理結果

### 5.8 隱私侵犯事件處理

#### 5.8.1 事件識別與報告

* 明確定義隱私侵犯事件的類型
* 建立內部報告機制
* 培訓員工識別與報告隱私侵犯事件
* 設置24小時內的初步報告要求
* 指定隱私侵犯事件接收與管理人員

#### 5.8.2 事件評估與分類

* 評估資料外洩的規模與性質
* 確定可能受影響的個人
* 評估對患者隱私的潛在影響
* 根據嚴重程度分類事件
* 決定是否需要通知監管機構或患者

#### 5.8.3 事件控制與緩解

* 立即採取行動控制事件
* 防止進一步的資料外洩
* 恢復資料安全性
* 移除外洩資料（如可行）
* 實施緩解措施減少傷害

#### 5.8.4 通知與溝通

* 依法向監管機構報告重大隱私侵犯事件
* 向受影響患者發出通知
* 提供清晰的事件描述與可能影響
* 告知已採取的措施
* 提供患者保護自身權益的建議

#### 5.8.5 事件調查與記錄

* 調查事件根本原因
* 記錄事件的完整細節
* 收集與保存相關證據
* 協助執法或監管調查（如適用）
* 準備詳細的事件報告

#### 5.8.6 後續改進措施

* 根據調查結果制定改進計劃
* 更新隱私保護措施
* 加強員工培訓
* 修改政策與程序
* 監控改進措施的實施與效果

### 5.9 教育訓練

#### 5.9.1 新進人員培訓

* 在入職培訓中納入隱私保護內容
* 介紹組織的隱私政策與程序
* 說明員工的責任與義務
* 提供常見隱私保護情境的實例
* 確保員工了解違規後果

#### 5.9.2 定期培訓與更新

* 至少每年進行一次隱私保護培訓
* 更新培訓內容反映法規與政策變化
* 針對新識別的風險提供額外培訓
* 分享隱私侵犯事件的經驗與教訓
* 使用多種培訓方式確保有效學習

#### 5.9.3 角色特定培訓

* 根據不同角色提供專業培訓
* 針對高風險角色(如系統管理員)提供強化培訓
* 為管理人員提供監督與管理培訓
* 為直接接觸患者的員工提供溝通技巧培訓
* 評估培訓效果並進行必要調整

#### 5.9.4 隱私意識提升

* 定期發送隱私保護提醒與最佳實踐
* 張貼隱私提示在關鍵區域
* 分享隱私保護成功案例
* 鼓勵員工提出隱私保護建議
* 建立隱私保護文化

### 5.10 監督與稽核

#### 5.10.1 常規監督

* 建立日常隱私保護監督機制
* 定期檢查資料存取記錄
* 監控異常的系統活動
* 進行隨機資料處理審查
* 執行治療環境隱私檢查

#### 5.10.2 內部稽核

* 至少每年進行一次隱私保護內部稽核
* 審查隱私政策與程序的執行情況
* 檢查資料保護措施的有效性
* 評估員工對隱私政策的遵守情況
* 提出改進建議

#### 5.10.3 外部評估

* 定期邀請外部專家評估隱私保護措施
* 參與行業隱私保護標準評估
* 根據評估結果進行改進
* 確保符合最新法規要求
* 與同業分享最佳實踐

#### 5.10.4 合規性評估

* 定期評估對相關法規的遵守情況
* 追蹤法規變化並更新政策
* 評估新服務或技術的隱私影響
* 記錄合規性評估結果
* 及時處理不合規問題

#### 5.10.5 報告與改進

* 定期向管理層報告隱私保護狀況
* 追蹤改進措施的實施進度
* 衡量隱私保護措施的效果
* 持續優化隱私保護程序
* 記錄並分享改進成果

## 6. 記錄

| 記錄名稱 | 記錄編號 | 保存期限 | 保管部門 |
| --- | --- | --- | --- |
| 患者隱私同意書 | PT-R-009-01 | 10年 | 物理治療部、病歷室 |
| 資料存取記錄 | PT-R-009-02 | 5年 | 資訊部門、病歷室 |
| 隱私侵犯事件記錄 | PT-R-009-03 | 10年 | 品質管理部、物理治療部 |
| 隱私保護培訓記錄 | PT-R-009-04 | 5年 | 人資部門、品質管理部 |
| 隱私保護稽核報告 | PT-R-009-05 | 7年 | 品質管理部 |
| 患者資料存取申請表 | PT-R-009-06 | 3年 | 病歷室、物理治療部 |
| 資料銷毀記錄 | PT-R-009-07 | 7年 | 病歷室、資訊部門 |

## 7. 相關文件

* QM-P001 文件控制程序
* QM-P002 記錄控制程序
* PT-P010 病歷管理程序
* IT-P001 資訊系統管理程序
* QM-P010 風險管理程序
* CS-P001 客戶滿意度調查程序
* PT-F006 患者隱私同意書
* PT-F007 患者資料存取申請表
* PT-F008 隱私侵犯事件報告表

## 8. 附件

* 附件1：患者隱私保護聲明樣本
* 附件2：患者資料存取流程圖
* 附件3：隱私侵犯事件處理流程圖
* 附件4：隱私風險評估清單
* 附件5：員工隱私保護責任聲明

## 9. 修訂紀錄

| 版本 | 修訂日期 | 修訂內容摘要 | 修訂人 | 審核人 | 批准人 |
| --- | --- | --- | --- | --- | --- |
| A | 2024/01/01 | 首次發布 | 品質主管 | 管理代表 | 院長 |