政策與程序	
標題： 保護受保護健康資訊/個人身份資訊	
部門政策所有者： 合規部	**政策編號：** HPA42
受影響的部門： 請勾選受本政策影響的所有部門	
☐ 行政部 ☐ 理賠部 ☐ 合規部 ☐ 客戶服務部 ☐ 對外事務部 ☐ 設施部 ☐ 財務部	☐ 人力資源部 ☐ 資訊技術部 ☐ 行銷部 ☐ 醫療管理部 ☐ 醫療服務提供者網絡部 ☐ 專案管理部 ☒ 全部
生效日期： 2019 年 5 月 15 日	**審查/修訂日期：** 2019 年 4 月、2020 年 12 月、 2021 年 4 月
委員會核准日期： PRC：2019 年 5 月、2020 年 7 月、 2021 年 4 月 合規委員會：2019 年 7 月	**廢除日期：**

產品類型： Medi-Cal	取代： IT15 – 工作站和電子存取的保護 IT18 – 應用程式日誌記錄程序 IT21 – 裝置和媒體控制 IT22 – 維持 ePHI 的完整性和安全性 IT33 – 電子郵件的使用 IT34 – 系統監控和活動審查 IT203 – 保護 ePHI HPA06 - 受保護健康資訊的行政保護措施 HPA26 - 受保護健康資訊的使用和披露 HPA27 司法程序披露 HPA28 出於執法目的的披露 HPA29 特殊政府職能的披露 HPA30 健康監督活動的披露 HPA31 - 保護屬於已終止或已故會員的受保護健康資訊 HPA32 向個人代表披露 HPA33 披露 PHI 的身份驗證 HPA36 會員 PHI 的披露 HPA38 向勞工賠償承運人披露 HPA39 受保護健康資訊的去身份化

I. 目的

Health Plan of San Joaquin (HPSJ) 應合理保護會員記錄中包含的受保護健康資訊 (PHI)，使其免遭《健康保險流通與責任法案》(HIPAA) 隱私和安全規則以及《醫療資訊保密法》(CMIA) 不允許的任何有意或無意使用或披露。本政策與程序 (P&P) 說明了為保護這些機密資訊而實施的隱私和安全控制。

II. 政策

A. Health Plan of San Joaquin 實施行政、實體和技術保護措施，以合理適當地保護 PHI 的機密性、完整性和可用性，包括根據 45 CFR 第 164.308、164.310、164.312 和 164.502(f) 節代表 DHCS 建立、接收、維護、使用或傳輸的電子 PHI，並防止在本協議規定之外使用或披露 PHI（DHCS 合約附錄 G，第 C.2 條）。

B. 除非在 45 C.F.R. § 164.508(b)(4) 中的有限情況下，HPSJ 不得以個人是否授權為條件提供治療、付款、入保或福利資格。

C. Health Plan of San Joaquin 將控制 PHI 的獲得並確保以適當的方式對其進行處理。如政策與程序 (P&P) CMP01 違規行為的應對和預防中所述，應親自、透過電子郵件或匿名方式向合規部報告違反本政策的行為。

D. Health Plan of San Joaquin 可能會向曾在去世前參與個人照護或健康照護付款的已故 HPSJ 會員的家庭成員披露與此人的參與相關的個人受保護健康資訊，除非這樣做與承保實體已知的個人先前表達的任何偏好不一致

E. 會員有權撤銷授權，前提是撤銷以書面形式提出，但 HPSJ 已根據授權行事除外。

F. Health Plan of San Joaquin 應遵守健康照護服務部門 (DHCS) 的合約，「僅在為 DHCS 執行或代表 DHCS 執行本協議規定的職能、活動或服務時使用或披露 PHI，前提是此類使用或披露將不得違反 HIPAA 規定」（DHCS 合約附錄 G.III.A）。

G. 合規長負責確保 PHI（包括敏感服務）的非常規披露是允許且必要的。Health Plan of San Joaquin 的持照健康照護人員瞭解 HIPAA 允許他們在未經會員許可的情況下披露 PHI 的活動

H. 電子通訊和傳輸

1. 員工必須在傳輸之前對包含機密資訊的電子郵件訊息進行加密。
2. 在透過公共網路（即網際網路）傳輸機密資訊時，員工必須使用加密通道、虛擬私人網絡 (VPN) 或安全檔案傳輸 (SFTP) 或安全套接層 (SSL) 等協議。

I. 電子媒體和儲存

1. Health Plan of San Joaquin 禁止將 PHI/ePHI 儲存在當地桌上型電腦硬碟上。
2. Health Plan of San Joaquin 必須對儲存在可攜式裝置和媒體（即筆記型電腦、可攜式存放媒體和磁帶）上的 ePHI 進行加密。
3. Health Plan of San Joaquin 必須在加密是適當且合理的情況下對包含 ePHI 的硬碟進行加密。在 HPSJ 經過仔細評估和考慮後確定加密是不適當或不合理的情況下，HPSJ 必須實施替代保護措施，以提供與加密相同等級的保護。
4. Health Plan of San Joaquin 必須監管包含 ePHI 的硬體、存放媒體和電子媒體的蹤跡。

5. Health Plan of San Joaquin 必須在重複使用包含 ePHI 的電子媒體前對其清除敏感資料。
6. Health Plan of San Joaquin 必須在處置包含 ePHI 的電子媒體前對其清除敏感資料或實體銷毀。

J. Health Plan of San Joaquin 的加密方法和程序必須使用符合 FIPS 140-2 的加密演算法。

K. 審核記錄和審查

1. Health Plan of San Joaquin 必須記錄用於建立、接收、維護或傳輸 ePHI 的資訊系統的活動。
2. Health Plan of San Joaquin 必須定期檢查用於建立、接收、維護或傳輸 ePHI 的資訊系統的活動和審核記錄。

L. 電腦和電子裝置

1. 用於建立、接收、維護或傳輸 ePHI 的電腦和電子裝置必須：
   a. 包含針對惡意軟體的保護，包括適用的關鍵作業系統修補程式、服務包或服務更新。
   b. 具有加密硬碟或透過補充可提供與加密等效保護的控制來得到保護。
   c. 在無活動狀態持續一段時間後自動鎖定。
   d. 僅限具有履行職責或職能所需的最低許可權的使用者和進程使用。
2. Health Plan of San Joaquin 必須在 IT 安全部或供應商通知後的 30 天內定期維護聯網電腦或電子裝置，包括應用關鍵安全修補程式。Health Plan of San Joaquin 按照正常維護時間表應用未指定為關鍵的其他修補程式，這些修補程式可能與上述修補程式不同。

III. 程序

A. 合規長（隱私長）和安全長應負責 PHI/ePHI 的行政保護措施。

a. 包含 PHI 的紙本文件。
   i. 包含 PHI 的文件將儲存在工作區域的上鎖機櫃中或安全位置。
   ii. 包含 PHI 的大量文件將以安全格式郵寄，並隨附追蹤和簽名要求。此資訊將按照記錄管理保留計畫進行維護和儲存。
   iii. 包含 PHI 的文件需根據 P&P CMP02 記錄管理和保留進行永久銷毀。

b. 口頭溝通
   i. 只能在適當的工作區域討論 PHI，而不能在集體/公共區域討論。
   ii. Health Plan of San Joaquin 會員訪談和討論將在安全區域進行（例如但不限於使用會員室）。

c. 電子通訊和傳輸
   i. 電子訊息（電子郵件）

      1. Health Plan of San Joaquin 使用電子郵件加密方法（即使用「Send Secure」桌面 Outlook 或「Protect」Office 365 Outlook 按鈕）對發送給 hpsj.com 域之外的收件者的電子郵件進行加密。

      2. 使用者不得在電子郵件的主題欄位中新增 PHI。

      3. 企業電子郵件系統會根據一組 PHI 標準審查和評估外發電子郵件訊息，並對任何符合這些標準的未加密訊息自動進行加密。

   ii. Health Plan of San Joaquin 使用加密通道或 VPN、SSL 或 SFTP 等協定進行電子通訊，或透過公共網路傳輸包含 ePHI 的檔案。如果供應商或合作夥伴不具備支援 SFTP 的能力時，HPSJ 會使用 PGP（Pretty Good Privacy）等應用程式對檔案進行加密，然後再透過未加密的通道進行傳輸。

   iii. Health Plan of San Joaquin 的員工和供應商/合作夥伴在透過公共網路傳輸 ePHI 的任何遠端使用者互動工作階段期間使用 VPN 或 Citrix。

   iv. 網路應用程式使用傳輸層安全 (TLS) 來確保透過作為 HTTPS 的 HTTP 傳輸的 ePHI 的真實性和完整性。

d. 電子媒體和儲存

   i. 資訊技術營運部制訂了確保可攜式媒體對儲存的資料自動進行加密的程序。

   ii. 需要儲存 ePHI 時，使用者會將 ePHI 儲存到網路磁碟中。

   iii. 資訊技術營運部會停用桌上型電腦的 USB 連接埠。

   iv. 使用者可以在獲得核准的情況下根據本政策請求寫入可攜式存放媒體的能力。

v. 資訊技術營運部會向授權啟用 USB 磁碟機的使用者發放自動加密的 USB 磁碟機。

vi. Health Plan of San Joaquin 會按照資訊技術營運部標準和程序的規定記錄所有包含 ePHI 的電子媒體的接收、部署和銷毀。

vii. 在將包含 ePHI 的電子媒體重複用於不同的系統或由不同的所有者重複使用之前，HPSJ 會根據資訊技術營運部標準和操作程序對其清除敏感資料或安全清除。

viii. 在處置之前，HPSJ 會根據資訊技術營運部標準和操作程序透過實體銷毀或清除敏感資料來安全銷毀所有包含（或懷疑包含）ePHI 的電子媒體。

e. 加密

i. Health Plan of San Joaquin 有在認為適當時對資訊進行加密和解密的機制。

ii. Health Plan of San Joaquin 使用以下因素來評估加密靜態資料的適當性和合理性：

1. 應用程式在具有加密磁碟機的伺服器上執行的能力
2. 應用程式或伺服器支援資料加密/解密機制的能力
3. 加密對應用程式效能和功能的影響
4. 執行或支援加密的額外資源成本

iii. 在 HPSJ 確定加密靜態資料是不合理或不適當的情況下，HPSJ 將執行以下所有補償控制或以下補償控制的組合：

1. 將伺服器安置在安全的伺服器機房或資料中心中
2. 記錄伺服器機房或資料中心的所有出入情況
3. 遵循加強伺服器的安全最佳實踐
4. 實現入侵偵測與防禦 (IDS/IPS) 或資料遺失防護 (DLP) 系統。

f. 審核記錄和審查

i. Health Plan of San Joaquin 資訊系統記錄活動，例如身份驗證嘗試失敗、設定變更、進程啟動、關閉或重新開機，以及惡意軟體或可疑活動偵測。

ii. Health Plan of San Joaquin 有審查日誌以發現未經授權存取的機制。

g. 電腦和電子裝置

i. Health Plan of San Joaquin 使用防火牆等週邊安全裝置保護可以獲得機密資訊的資訊資源。

ii. 資訊技術部向電腦分配對停用的可攜式存放媒體進行寫入或存取的能力。

iii. 電腦包括防止惡意軟體（即防毒軟體）的軟體以及安裝新版本作業系統 (OS) 安全和關鍵更新的機制。

iv. 資訊技術部制訂了管理漏洞和修補程式的政策與程序。Health Plan of San Joaquin 基於風險的關鍵修補程式優先排序方法可確保及時適當地應用修補程式，以解決應用程式、系統和網路裝置漏洞。

v. 可以獲得 ePHI 的電腦和電子裝置會在 10 分鐘無活動（閒置時間）後自動啟用受密碼保護的螢幕保護裝置程式。

h. 從會員或個人代表處獲得授權

i. 在收到 III.A. 中所述的請求後，會員必須填寫授權書。會員可以透過郵件提交授權書，也可以在 HPSJ 辦公室填寫授權書。Health Plan of San Joaquin 的員工可以透過網際網路/表格/HIPAA 獲得授權書。授權書必須是單獨的文件，不得與其他任何類型的表格組合。

ii. 授權書將僅透過我們會員資料庫中目前儲存的地址郵寄給會員。嚴禁將授權書郵寄到其他地址。

iii. 在 HPSJ 辦公室填寫授權書時，客戶服務部工作人員會要求 HPSJ 會員提供相片身份證明並記錄在通話日誌中。

iv. 如政策 HPA32 向個人代表披露中所述，非 SPD 會員的個人代表必須提交或出示其合法授權證明才能為會員填寫授權書。有效證明的範例包括：身體或精神殘障會員證明個人代表是父母的出生證明、表明允許個人代表為會員尋求和獲得醫療照護的法院或郡縣文件、授權個人代表代表會員行事的授權委託書，或將個人代表指定為看護人員的看護人員授權宣誓書。

i. 如果身體或精神上無行為能力，SPD 會員無需填寫授權書。工作人員可以使用 DHCS 提交並儲存的資料來識別個人代表。其他所有證明必須得到合規部的核准。

j. 如果 HPSJ 必須尋求會員或個人代表的授權，HPSJ 人員將填寫授權書的所有部分，然後再提供給會員或其個人代表進行簽名。

k. 如果 HPSJ 尋求會員或個人代表的授權，將向會員或個人代表提供一份已簽署的授權書副本。如果會員或個人代表尋求授權，可應要求提供副本。

l. Health Plan of San Joaquin 可能會在以下情況下披露已故個人的 PHI。

   i. 對於已故會員，如果在會員去世後 50 年內請求獲得 PHI，HPSJ 應將執行人、管理人或有權代表已故會員行事的其他人視為其個人代表。此類代表必須提供佐證其合法授權的法律文件。
   ii. 在懷疑死亡是由犯罪行為導致時，披露給執法部門以提醒其注意個人的死亡。
   iii. 僅對死者的 PHI 進行研究。
   iv. 披露給器官勸募組織或其他從事屍體器官、眼睛或組織的勸募、儲存或移植的實體，以促進器官、眼睛或組織的捐贈和移植。
   v. 披露給家庭成員或在個人去世前參與過個人健康照護或照護付款的其他人，除非這樣做與 HPSJ 已知的已故個人先前表達的任何偏好不一致。

m. 授權審查

   i. 提交的所有 HPSJ 授權書均由客戶服務部在按照授權書指示的方式使用或披露會員 PHI 之前進行審查。

   ii. 所有非 HPSJ 授權書均由合規部在按照授權書指示的方式使用或披露會員 PHI 之前進行審查。在以下任一情況下，授權書將被視為不合格且無效：

      1. 授權書要求出於與 Medi-Cal 計畫管理無關的目的披露會員的 PHI。

      2. 授權書由未成年人的個人代表（例如父母）簽署，但按照《加州家庭法》的規定，只能在未成年人許可時使用或披露 PHI。

3. 授權書上的任何內容不完整。

4. 到期日期已過或 HPSJ 獲悉發生了到期事件。

5. 會員後來撤銷了有效的授權書。

6. Health Plan of San Joaquin 獲悉授權書中提供的任何重要資訊是虛假資訊。

iii. 會員或其個人代表指出的任何限制或禁令，包括與敏感服務相關的限制或禁令，均由合規部記錄在會員模組的個人代表和提醒部分中。

n. 授權撤銷

i. 會員或個人代表有權隨時撤銷授權。撤銷必須以書面形式提出。

ii. Health Plan of San Joaquin 會採取一切必要措施來履行和遵守撤銷，除非 HPSJ 已據此採取行動。

o. 文件

i. 當 HPSJ 徵求授權時，會向會員或個人代表提供一份已簽署的授權書副本。

ii. 合規部保留所有有效或無效的授權書以及任何後續撤銷書。

iii. 授權書和撤銷書根據 CMP02 記錄管理和保留進行保留。

iv. 特殊政府職能

v. 申請由合規部審查和回覆。

vi. 接受的申請僅限於 45 CFR 164.512(k) 授權的申請。

vii. 合規部透過要求提供適當的身份證明來驗證在 HPSJ 場所申請獲得會員 PHI 的官員。

viii. 合規部使用標有「機密」的信封或透過傳真將資料郵寄給官員

IV. 附件

A. 術語表連結

V. 參考資料

a. 45 CFR 第 §160 和 §162 部分
b. 45 CFR 164.308 (a)(1)(ii)(D) - 資訊系統活動審查
c. 45 CFR 164.310(d)(1) – 裝置和媒體控制
d. 45 CFR 164.310(d)(2)(i) - 處置
e. 45 CFR 164.310(d)(2)(ii) – 媒體重複使用
f. 45 CFR 164.310(d)(2)(iii) – 問責制
g. 45 CFR 164.312(b) - 審核控制
h. 45 CFR 164.312(e)(1) – 傳輸安全
i. 45 CFR 164.312(e)(2)(i) – 完整性控制
j. 45 CFR 164.312(e)(2)(ii) – 加密
k. 45 CFR 164.312(a)(2)(iv) – 加密和解密
l. 45 CFR 164.502(f)
m. 《加州民法典》56 (CMIA)
n. CMP01 違規行為的應對和預防
o. CMP02 記錄管理和保留
p. 合規（內部審核和風險管理）專案計畫
q. 健康照護服務部門合約附錄 G，第 C.2. 條
r. FIPS PUB 140-2 – 加密模組安全要求
s. 《健康資訊技術促進經濟和臨床健康法案》（HITECH 法案）
t. HPA08 緩解
u. HPA33 身份驗證
v. HR11 修正措施
w. IT33 電子郵件
x. 美國國家標準技術研究所特別出版物 (SP) 800-53 版次 4，聯邦資訊系統和組織的安全和隱私控制

VI. 監管機構核准

根據 HPSJ 與健康照護服務部門 (DHCS) 達成的協議，HPA42 因接受審查超過 60 天而被核准實施。

VII. 修訂記錄

狀態	修訂日期	修訂摘要
提議	2019 年 1 月 31 日	結合了現有政策的內容，並新增了內容以符合 HIPAA 安全規則
定稿	2019 年 4 月 2 日	經 PSOC 核准
修訂	2020 年 1 月 13 日	新增了政策與程序術語表
修訂	2020 年 2 月 10 日	將 HPA06 行政保護措施和 HPA31 已故會員的 PHI 保護的部分內容合併到 IT203 中。 將政策標題從 IT203 改為 HPA42，將政策所有者從資訊技術部改為合規部。合併和更新了目的、政策和程序。合併了參考資料。
修訂	2020 年 2 月 25 日	變更了格式和標題。
修訂	2020 年 12 月 11 日	將政策 HPA26 合併到 HPA42 中。AG
修訂	2021 年 4 月 5 日	審查了政策的準確性。