

政策与程序	
政策编号和标题: HPA03 隐私官和安全官的指定	
主要政策所有者: 合规部	政策编号: HPA03
受影响/次要政策所有者: 选择负责遵守所述全部或部分政策或程序的部门	
1) <input checked="" type="checkbox"/> 所有部门 2) <input type="checkbox"/> 行为健康部 (BH) 3) <input type="checkbox"/> 福利管理部 (BA) 4) <input type="checkbox"/> 护理管理部 (CM) 5) <input type="checkbox"/> 索赔部 (CLMS) 6) <input type="checkbox"/> 社区市场与会员参与部 (MAR) 7) <input type="checkbox"/> 合规部 (CMP/HPA) 8) <input type="checkbox"/> 配置部 (CFG) 9) <input type="checkbox"/> 医疗服务提供者签约部 (CONT) 10) <input type="checkbox"/> 文化与语言部 (CL) 11) <input type="checkbox"/> 客户服务部 (CS)	12) <input type="checkbox"/> 设施部 (FAC) 13) <input type="checkbox"/> 财务部 (FIN) 14) <input type="checkbox"/> 人力资源部 (HR) 15) <input type="checkbox"/> 信息技术/核心系统部 (IT) 16) <input type="checkbox"/> 药房 (PH) 17) <input type="checkbox"/> 医疗服务提供者网络部 (PRO) 18) <input type="checkbox"/> QI 健康公平部 (GRV/HE/HEQ/PHM/QM) 19) <input type="checkbox"/> 使用管理部 (UM)
产品类型: <input checked="" type="checkbox"/> Medi-Cal	取代政策编号: 无

I. 目的

概述作为 Health Plan of San Joaquin 和 Mountain Valley Health Plan（简称为“Health Plan”）运营和开展业务的 San Joaquin 县健康委员会（简称为“委员会”）的隐私官¹和安全官²的角色和职责。

¹ 45 CFR §164.530(a),

² 45 CFR §164.308 (a)(2)。

II. 政策

A. 隐私官

1. 首席合规官 (CCO) 是 Health Plan 指定的隐私官。
2. 隐私官或其指定人员负责制定和实施 Health Plan 的 HIPAA 政策与程序 (P&P)，其中包括提出 P&P 相关投诉的方法。³
3. 隐私官或其指定人员是负责接收、处理和记录投诉的联系人。
4. 隐私官或其指定人员负责提供有关受保护健康信息 (PHI) 隐私惯例通知 (NPP) 所涵盖事项的信息。⁴
5. 本 P&P 记录了隐私官和安全官的人员指定，其中安全官的人员指定在下一节 (B.1.) 中。⁵
6. 对系统安全性进行定期内部审计和风险评估，以防止电子受保护健康信息泄漏。
7. 隐私官管理 Health Plan 的活动，以确保遵守与会员信息相关的联邦和州隐私法规，包括但不限于健康保险流通与责任法案 (HIPAA)、HIPAA 违规通知规则、医疗信息保密法 (CMIA) 以及国家品质保证委员会 (NCQA) 的隐私和保密职能。

B. 安全官

1. 核心系统支持总监是指定的 Health Plan 安全官。
2. 安全官或其指定人员负责制定和实施 HIPAA 安全 P&P。⁶
3. 安全官或其指定人员负责管理 Health Plan 的活动，以确保遵守与会员信息相关的联邦和州安全法规，包括但不限于 HIPAA 安全规则。

³ 45 CFR §164.530(d)

⁴ 45 CFR §164.520

⁵ 45 CFR §164.530(a)(2)

⁶ 45 CFR §164.308(a)(2)

III. 程序

A. 隐私官或其指定人员负责如下所述实施隐私政策：

1. 制定 P&P 并监督其初始实施和后续修订，旨在遵守相关隐私、保密和违规通知法规，其中包括 HIPAA 和 CMIA。至少每年审查一次 HIPAA P&P。
 - a. 根据 P&P CMP24 合规计划培训和教育，准备对所有 Health Plan 员工和其他适用的第三方实体进行培训。隐私官应根据需要提供额外培训。
 - b. 隐私官与医疗服务提供者网络合作，要求 Health Plan 的第三方实体遵守 Health Plan 政策与程序，包括确保对员工和分包商进行培训和教育。
2. 接收会员、Health Plan 员工和其他第三方实体有关违反隐私和安全 P&P 的投诉。
3. 编制和维护 NPP 以及供会员在行使 NPP 中所述权利时使用的表格。协助客户服务部向会员澄清 NPP 中定义的权利。
4. 审查所有供应商合同，并确保接收 PHI 的任何供应商在披露 PHI 之前，根据合同协议、P&P 以及有关业务伙伴和其他适用第三方实体的州和联邦法规签署数据使用协议 (DUA)、数据共享协议 (DSA) 或业务伙伴协议 (BAA)。
5. 担任隐私和安全监督委员会 (PSOC) 的主席或指定安全官担任主席。
6. 监督对 Health Plan 员工进行的定期审计和测试，以衡量是否符合 HIPAA P&P。
7. 编制隐私和安全意识提醒，并分发给 Health Plan 的员工和适用的第三方实体。
8. 与安全官合作处理与 HIPAA 隐私和安全相关的所有事务，其中包括 P&P 更新和修订。

B. 安全官或其指定人员负责如下所述实施安全政策：

1. 制定和实施 P&P，旨在遵守相关安全法规，其中包括 HIPAA。至少每年审查一次 P&P。
2. 每年对包含电子受保护健康信息的系统进行一次风险评估。

3. 根据安全规则标准，为应对影响电子受保护健康信息 (ePHI) 安全的环境或运营变化，需定期进行技术和非技术评估，以确定 Health Plan 的安全 P&P 是否满足 HIPAA 安全规则的要求。
4. 在隐私官指定时担任 PSOC 主席。
5. 监督对 Health Plan 员工进行的定期审计和测试，以衡量是否符合安全 P&P。
6. 与隐私官合作处理与 HIPAA 隐私和安全相关的所有事务，其中包括 P&P 更新和修订。

IV. 附件

- A. DHCS Medi-Cal 管理式护理计划定义（附录 A，附件 I，1.0 定义）
- B. [术语表链接](#)
- C. Medi-Cal 管理式护理合同缩略语列表（附录 A，附件 I，2.0 缩略语）

V. 参考资料

- A. 45 CFR 第 §160、§162 和 §164 部分 HIPAA 法规
- B. 45 CFR §164.308(a)(2)、45 CFR §164.520 和 45 CFR §164.530
- C. 《加州民法典》(CIV) §56 - §56.37 CMIA
- D. CMP24 合规计划培训和教育
- E. DHCS 合同附录 G 业务伙伴附录
- F. HEALTH PLAN 合规计划
- G. 健康信息技术促进经济和临床健康法案（HITECH 法案）
- H. HPA05 业务伙伴
- I. HPA09 HEALTH PLAN 针对隐私和安全规则违反行为的员工纪律处分
- J. 诺克斯-基恩法案 §1352

VI. 修订记录

版本	修订摘要	日期
001	进行年度审查，将 P&P 置于当前模板中，进行了少量编辑、语法和格式更改，更新了参考资料和附件部分。	2023 年 10 月 30 日
002		
003		
初始生效日期：2002 年 1 月 7 日		

VII. 委员会审查和批准

委员会名称	版本	日期
合规委员会	001	2024 年 2 月 15 日
<ul style="list-style-type: none"> • 隐私与安全监督委员会 (PSOC) 	001	2023 年 12 月 11 日
<ul style="list-style-type: none"> • 计划完整性委员会 		
<ul style="list-style-type: none"> • 审计与监督委员会 		
<ul style="list-style-type: none"> • 政策审查委员会 	001	2023 年 12 月 20 日
质量与使用管理委员会		
<ul style="list-style-type: none"> • 质量运营委员会 		
<ul style="list-style-type: none"> • 申诉委员会 		

VIII. 监管机构批准

部门	审查者	版本	日期
健康护理服务部 (DHCS)	无	无	无
管理式护理部 (DMHC)	无	无	无

IX. 批准签名

签名	姓名 职务	日期
	PRC 主席	
	政策所有者	
	部门主管	
	首席执行官	

*签名已存档，不会出现在已发布的副本上