| 政策与程序 | |
|---|---|
| **政策编号和标题：**<br>HPA07 报告和缓解可疑的隐私与安全事件及违规行为 | |
| **主要政策所有者：**<br>合规部 | **政策编号：**<br>HPA07 |
| **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) ☒所有部门<br>2) ☐会计与财务部 (FIN)<br>3) ☐行政管理部 (ADM)<br>4) ☐护理管理部 (CM)<br>5) ☐索赔部 (CLMS)<br>6) ☐社区市场与会员参与部 (MAR)<br>7) ☐合规部（CMP 和 HPA）<br>8) ☐配置部 (CFG)<br>9) ☐文化与语言部 (CL)<br>10)☐客户服务部 (CS) | 11)☐设施部 (FAC)<br>12)☐HEDIS/NCQA (QI)<br>13)☐人力资源部<br>14)☐信息技术/核心系统部 (IT)<br>15)☐药房 (PH)<br>16)☐项目管理办公室<br>17)☐医疗服务提供者签约部 (CONT)<br>18)☐医疗服务提供者服务部 (PS)<br>19)☐质量管理部 (QI)<br>20)☐使用管理部/BH (UM) |
| **产品类型：**<br>☒Medi-Cal | **取代政策编号：**<br>HPA08 |

## I. 目的

概述处理隐私或安全事件、与受保护健康信息/个人信息 (PHI/PII) 相关的违规行为和/或其他擅自访问、使用或披露 PHI/PII 的行为的报告和缓解流程。

## II. 政策

A. 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"）必须根据《健康保险流通与责任法案》(HIPAA)、隐私、安全和违规通知规则、45 CFR 第 160 和 164 部分、《加州民法典》第 1798.29 部分以及合同或监管要求，立即将可疑或确认的隐私或安全事件、与 PHI/PII 相关的违规行为以及其他擅自访问、使用或披露 PHI/PII 的行为（统称为"HIPAA 事件"）报告给监管机构。

B. 隐私官或指定人员和/或 IT 安全官必须将 HIPAA 事件报告给隐私和安全监督委员会 (PSOC) 以及相应的联邦和州机构。

C. 下面是报告事件的方法：SharePoint 链接、主管、经理或执行团队、合规团队成员，通过传真、电子邮件、电话、匿名或通过现场合规举报信箱。

D. Health Plan 必须根据本政策将不当 HIPAA 事件的书面报告提供给 DHCS。

E. Health Plan 将使用 DHCS 门户网站将可疑的 HIPAA 事件报告给 DHCS。Health Plan 将通知个人会员，其 PHI/PII 已因或认为已因 DHCS 确定的违规行为而被访问、获取、使用或披露。
F. Health Plan 不得要求个人放弃其权利作为提供治疗、付款、投保健康计划或符合福利资格的条件。[1]
G. 如果执法官员声明通知、通告或公布会妨碍刑事调查或对国家安全造成损害，则 Health Plan 必须延迟通知。[2]
H. Health Plan 的计划完整性部门在隐私官和 IT 安全官的监督下负责本政策的监管和执行。
I. 合规官和隐私监督委员会每年都会审查一次本政策，并在必要时进行修订。

## III. 程序

A. 发现

违规行为必须视为自 Health Plan 任何工作人员或任何其他 Health Plan 代理人（实施违规行为的人员除外）怀疑或知晓其存在，或通过合理履行职责即可怀疑或知晓其存在的第一天起就已被发现。

1. Health Plan 的员工必须在发现任何 HIPAA 事件后立即通过以下方法报告：
    a. 直接通过 Share Point Link 进行报告，Share Point Link 是链接到 https://secure.compliance360.com 的在线报告应用程序。
    b. 直接向工作人员的主管、经理或执行团队成员报告。
    c. 直接向 Health Plan 的隐私办公室或安全官报告。
    d. 直接向任何合规管理团队成员报告。
    e. 通过电子邮箱 PIU@HPSJ.com 报告。
    f. 通过传真 (209) 762-4721 报告。
    g. 通过 Syntrio:Lighthouse Reporting 上的匿名在线报告应用程序报告
    h. 通过位于 Health Plan 设施内的合规举报信箱报告。
    i. 通过合规热线 1-800-822-6222 报告。
    j. 管理团队成员。

[1] 45 CFR § 164.530(h)
[2] 45 CFR §164.412

2. Health Plan 的部门和员工应在发现可疑的隐私或安全事件或违规行为后立即使用上述方法中的一种向合规部报告。若不报告，将构成违反政策与程序的行为。
3. Health Plan 的员工必须与合规部合作，按要求调查和补救 HIPAA 事件并遵守以下要求。
    a. 在调查期间遵守“隐私事件补救要求的服务水平协议”中概述的流程和时间表。
    b. 遵守隐私事件的办公级程序合规性和企业主补救流程中概述的补救角色和职责。
    c. 若不遵守，可能会导致根据 HPA09 HPSJ 员工处分采取适用的纪律处分。
4. 医疗服务提供者、承包商、分包商、下游分包商（包括业务伙伴）（统称为“第三方”）应立即通过以下方式报告：
    a. 通过电子邮件通知地址 incidents@dhcs.ca.gov。第三方需要通过同一电子邮件抄送至 Health Plan 的 PIU 收件箱 piu@hpsj.com。
    b. 通过电话 (866) 866-0602
    c. 当使用门户网站或电话报告方法时，第三方需要通过 Health Plan 的 PIU 收件箱电子邮件地址 piu@hpsj.com 立即发送通讯，提供与事件相关的相同信息。
5. 第三方报告要求
    a. HPA05 – 业务伙伴中涵盖了有关第三方报告义务的更多详细信息。
    b. Health Plan 告知并教育第三方 BAA 中所述的报告义务。
    c. 如果第三方未能及时报告，Health Plan 将在得知此类事件后 24 小时内代表第三方将事件报告给 DHCS。
    d. 如果第三方未能遵守后续报告要求，Health Plan 还要根据后续报告要求履行职责。
    e. 如果第三方未能遵守 BAA 中所述的监管报告要求，可能会导致 Health Plan 评估的处分，其中可能包括终止合同。

B. Health Plan 会员报告

1. 会员可以通过电话或邮件向客户服务代表提出 HIPAA 违规投诉。隐私惯例通知提供了邮寄地址和电话号码。会员还可以通过我们的公共网站 Syntrio:Lighthouse Reporting 提交投诉。
2. Health Plan 会按照本政策所述的方式处理投诉。

C. 向监管机构报告 HIPAA 事件

1. Health Plan 的合规部必须根据以下准则调查、通知和报告发现的 HIPAA 事件：
2. 违规行为：
    a. 如果发现保存在电脑上的 PHI/PII 存在安全漏洞，并且 PHI/PII 已被或有理由认为已被未经授权的人员获取，或者发现可疑的隐私或安全事件，并且该事件涉及社会保障局向 DHCS 提供的数据，则合规部必须**立即**通过 DHCS 门户网站通知 DHCS。
    b. 使用 DHCS 隐私事件报告 (PIR) 模板通知 DHCS 合同经理、DHCS 隐私官和 DHCS 信息安全官。
3. 可疑的 HIPAA 事件：
    a. **在 24 小时内**，通过 DHCS 门户网站通知任何可疑的隐私或安全事件、入侵或违反 Health Plan 与 DHCS 签订的 2024 年 DHCS 合同擅自访问、使用或披露 PHI 或 PII 的行为。
4. 调查：
    a. 在发现 HIPAA 事件后，合规部将立即启动调查。
    b. 在发现后 **72 小时**内，通过 DHCS 门户网站提交调查最新进展。
    c. 在发现违规行为或擅自使用或披露后**十 (10) 个工作日**内，通过 DHCS 门户网站提交完整的 PIR 详细信息。如果需要更多时间才能完成调查，则 Health Plan 将请求 DHCS 延期，并在延期期间向 DHCS 提交每周最新进展，直至调查完成。 在发现 HIPAA 事件后，Health Plan 必须：
        i. 及时采取纠正措施，以减轻与违规行为相关的任何风险或损害，并保护运营环境。
        ii. 按照适用的联邦和州法律法规的要求采取任何与此类擅自披露相关的行动。
5. 通知会员：
    a. 如果个人的 PHI 已因或有理由认为已因此类违规行为而被访问、获取、使用或披露，Health Plan 必须通知涉及的每个人。
    b. 通知必须及时发出而不得无故拖延，并且在任何情况下不得晚于发现违规行为后 60 个日历日。
    c. DHCS 必须审查并批准通知内容。

6. 通知媒体：
    a. 如果违规行为涉及超过五百 (500) 个人的不安全 PHI，需要通知媒体。
    b. 通知必须及时发给媒体而不得无故拖延，并且在任何情况下不得晚于发现违规行为后六十 (60) 个日历日。
7. 通知美国卫生与公共服务部 (DHHS) 部长、民权办公室：
    a. 如果违规行为涉及超过五百 (500) 个人的不安全 PHI，需要通知 DHHS 部长。
    b. 如果违规行为涉及少于五百 (500) 个人的不安全 PHI，Health Plan 必须保留此类违规行为的日志或其他文件，并且在不晚于每个日历年结束后六十 (60) 天内，将该日志提供给 DHHS 部长。

D. 确定哪些 HIPAA 事件可报告给 DHCS，哪些 HIPAA 事件不可报告给 DHCS。
1. 合理确认的所有违规行为都必须报告给 DHCS，但是，并非所有 HIPAA 事件都属于违规行为。 有以下三种例外情况：
    a. 无意获取、访问或使用
    b. 无意中透露给授权人员
    c. 无法保留 PHI。
    d. “HPSJ PIR 决策树”是确定哪些隐私或安全事件应分类为可报告给 DHCS 和不可报告给 DHCS 的指南。

E. 执法延迟
1. 如果执法官员向 Health Plan 声明要求的通知、通告或公布会妨碍刑事调查或对国家安全造成损害，则 Health Plan 必须：
    a. 如果声明为书面形式并指定了需要延迟的时间，则在官员指定的期限内延迟此类通知、通告或公布；或
    b. 如果声明为口头形式，Health Plan 将记录该声明，包括做出声明的官员的身份，并暂时延迟通知、通告或公布，延迟时间不得超过口头声明之日起 30 天。[3]

## IV. 附件。

A. DLP - 隐私事件的合规性和企业主补救流程。
B. DHCS Medi – Cal 管理式护理计划定义（附录 A，附件 I，1.0 定义）
C. DHCS 隐私事件报告
D. 术语表链接

[3] 45 CFR §164.412

E. 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）
F. 隐私事件补救要求的 SLA

## V. 参考资料

A. 45 CFR 第 §160、§162 和 §164.412 部分
B. 《加州民法典》§56 - §56.37 医疗信息保密法
C. CMP01 违规行为的应对和预防
D. CMP DP009 隐私事件登记和报告
E. DHCS 合同附录 G
F. HPA01 隐私和安全监督委员会 (PSOC)
G. HPA09 HPSJ 员工处分
H. HPSJ 业务伙伴协议
I. HPSJ PIR 决策树
J. Medi-Cal 隐私惯例通知
K. 隐私事件常见问题解答
L. 隐私事件补救要求的 SLA

## VI. 修订记录

*版本 001 自 2023 年 1 月 1 日起生效

| 版本* | 修订摘要 | 日期 |
|---|---|---|
| 000 | 2003 年 3 月、2003 年 7 月、2005 年 4 月、2009 年 1 月、2009 年 5 月、2012 年 6 月、2014 年 9 月、2018 年 11 月、2020 年 6 月、2020 年 7 月、2020 年 12 月、2021 年 2 月、2021 年 11 月、2022 年 10 月、2022 年 12 月、2023 年 2 月 | 无 |
| 001 | 将 HPA07 移至新的 2023 年模板中 | 2023 年 3 月 21 日 |
| 002 | 在 B. 部分"向 HPSJ 报告隐私或安全事件或违规行为"中输入了有关隐私事件补救要求的 SLA 的信息 | 2023 年 5 月 23 日 |
| 003 | 修订了业务伙伴报告违规行为的程序。 | 2023 年 7 月 14 日 |
| 004 | 根据 2024 年 DHCS 合同，在政策中新增了有关业务伙伴缓解违规行为和安全事件的内容。 | 2023 年 8 月 30 日 |
| 005 | 更改了内容格式以提高可读性。 | 2023 年 9 月 21 日 |
| **初始生效日期：** 2003 年 4 月 14 日 | | |

## VII. 委员会审查和批准

| 委员会名称 | 版本 | 日期 |
|---|---|---|
| 合规委员会 | 005 | 2023 年 12 月 7 日 |
| • 隐私与安全监督委员会 (PSOC) | 005 | 2023 年 11 月 7 日 |
| • 计划完整性委员会 | | |
| • 审计与监督委员会 | | |
| • 政策审查委员会 | 005 | 2023 年 11 月 15 日 |
| 质量与使用管理委员会 | | |
| • 护理质量委员会 | | |
| • 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