PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY / PROCEDURE

<table>
<tr><td colspan="3">Policy/Procedure Number: CMP-18 (Formerly ADM-20)</td><td colspan="3">Lead Department: Administration</td></tr>
<tr><td colspan="3">Policy/Procedure Title: Reporting Privacy Incidents and Breach Notifications</td><td colspan="3">☒ External Policy
☒ Internal Policy</td></tr>
<tr><td colspan="2">Original Date: 05/01/2009</td><td colspan="4">Next Review Date: 11/21/2025
Last Review Date: 11/21/2024</td></tr>
<tr><td>Applies to:</td><td>☒ Medi-Cal</td><td>☐ Healthy Kids</td><td colspan="3">☒ Employees</td></tr>
<tr><td rowspan="2">Reviewing Entities:</td><td>☐ IQI</td><td>☐ P & T</td><td colspan="3">☐ QUAC</td></tr>
<tr><td>☐ OPERATIONS</td><td>☐ EXECUTIVE</td><td>☒ COMPLIANCE</td><td colspan="2">☐ DEPARTMENT</td></tr>
<tr><td rowspan="2">Approving Entities:</td><td>☐ BOARD</td><td>☒ COMPLIANCE</td><td>☐ FINANCE</td><td colspan="2">☐ PAC</td></tr>
<tr><td>☐ CEO ☐ COO</td><td>☐ CREDENTIALING</td><td colspan="3">☐ DEPT. DIRECTOR/OFFICER</td></tr>
<tr><td colspan="3">Approval Signature: Sonja Bjork, CEO</td><td colspan="3">Approval Date: 11/21/2024</td></tr>
</table>

I. RELATED POLICIES:

A. CMP-13 Permitted Use, Disclosure, and Minimum Necessary Use of Member Information
B. CMP-23 External PHI Release Control
C. CMP-24 Physical and Administrative Safeguards
D. CMP-26 Verification of Caller Identity and Release of Information
E. CMP-41 Wellness and Recovery Program Records

II. IMPACTED DEPTS.:

All.

III. DEFINITIONS:

A. Date of Discovery: is the first day on which the incident or potential breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person who caused the incident or committed the breach) who is an employee, officer or agent of Partnership.
B. Privacy Breach: A privacy incident in which it is confirmed that Protected Health Information (PHI) has been compromised by an impermissible use or disclosure.
C. Privacy Incident Report: A report which contains details of a privacy issue involving Partnership members and their PHI.
D. Privacy Incident: An event or action that may have resulted in the unauthorized acquisition, access, use or disclosure of protected information in a manner not permitted under federal or state privacy laws.
E. Protected Health Information: The Privacy Rule issued by the U.S. Department of Health and Human Services protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Pursuant to 45 CFR §160.103, "Individually identifiable health information" is information, including demographic data, that relates to:
    a. The individual's past, present or future physical or mental health or condition,
    b. The provision of health care to the individual, or
    c. The past, present, or future payment for the provision of health care to the individual,

And that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. For the purposes of this policy, Protected Health Information (PHI) is any information that can be used to identify a Partnership member, including but not limited to the following identifiers:
    a. Name
    b. Member address (all geographic subdivisions smaller than a state)
    c. Dates directly related to an individual: including birth date, admission date, discharge date,

date of death

d. Telephone and/or fax number
e. Driver's License Number
f. Email Address(es)
g. Social Security Number (SSN)
h. Medical Record Number (MRN)
i. Health Plan Beneficiary Number (such as a Client Identification Number [CIN], or other health insurance policy or subscriber number)
j. Account Number
k. Any vehicle or device serial number, including license plates
l. Photographic images
m. Any other unique identifying number, characteristic, or code
n. Age greater than 89 (which identifies a smaller and easier to identify population)
o. Medical or Histories (medical history, treatment or diagnosis, mental or physical health condition, application and claims history, as well as appeals records)
p. Licensing Records (including Certificate/License Number)

E. Unsecured or unprotected PHI: PHI that is rendered usable, readable, or decipherable, in any form, to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS.

F. Partnership Workforce Member: For the purposes of this policy, "workforce member" is defined as a(n) Partnership HealthPlan of California (PHC) employee, volunteer, temporary personnel, intern, health care provider, subcontractor, delegate, and/or member of the Partnership Board of Commissioners employed by or acting on the behalf of Partnership.

IV. ATTACHMENTS:

N/A

V. PURPOSE:

To establish the process for which Partnership workforce members report potential or actual privacy issues to Partnership's Privacy Officer and provide guidance for breach notifications in the event a privacy breach has been determined.

VI. POLICY / PROCEDURE:

A. Policy:

1. Partnership is required to implement processes to support the discovery and reporting of incidents or breaches involving protected health information (PHI).
2. Partnership shall not engage in any act that may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against a member of the Partnership workforce who reports a privacy incident under this policy.
3. In compliance with DHCS Medi-Cal Contract 23-30236, Exhibit G, Business Associate Addendum (7-7.1): all Partnership workforce including but not limited to employees, volunteers, temporary personnel, interns, health care providers, subcontractors, delegates, and members of the Partnership Board of Commissioners, who access or disclose DHCS PHI, must complete information privacy and security training at least annually, and are notified of their obligation to immediately report potential or actual privacy incidents.
4. Partnership Workforce shall not take it upon themselves to determine at the point of discovery whether an incident is deemed a breach.
5. Privacy incidents may also be identified through member and provider grievances, Partnership's Compliance Hotline, or direct reports to Partnership's Privacy Officer, or designee.

B. Procedure

1. Reporting HIPAA Privacy Incidents to RAC or Partnership's Privacy Officer

Reporting Privacy Incidents

a. Upon discovery, Partnership Workforce Members, are required to immediately report all potential or actual HIPAA privacy incidents to Regulatory Affairs and Compliance (RAC) or Partnership's Privacy Officer.

b. Potential or actual incidents shall be reported immediately to RAC or Partnership's Privacy Officer by:

i. Internal workforce: Completing a referral using the EthicsPoint Incident Reporting Form (accessible through Partnership's intranet, PHC4Me; or

ii. External entities: Completing a referral using Partnership's Incident Reporting form (available on Partnership's external website www.partnershiphp.org) and submitting the completed form by email to RAC_Reporting@partnershiphp.org; or

iii. By calling the toll-free Compliance Hotline number at (800) 601-2146, anonymously, or

iv. Contacting any member of Partnership management, RAC, or the Partnership Privacy Officer.

c. Incident reports must contain all information known to the reporting party at the time of discovery.

d. The reporting party shall submit the incident immediately upon initial discovery. The completed form should contain all information requested known to the individual reporting the incident and shall include the date of initial discovery by Partnership or, any member of Partnership's workforce. Additional information, attachments and/or updates on previously reported incidents, may also be submitted through any of the previously mentioned reporting mechanisms.

2. Reporting 42 CFR Part 2 Incidents

a. Providers contracted with Partnership through the Wellness and Recovery Program for the provision of substance use disorder treatment services are considered Covered Programs as defined in 42 CFR Part 2, and as such, shall comply with Part 2 privacy reporting requirements and consistent with Partnership policy and procedure CMP-41 Wellness and Recovery Program Records.

3. Partnership's Regulatory Reporting Requirements

a. Pursuant to DHCS Contract 08-85215, Exhibit G, Provision J, Partnership PHC maintains processes to support the identification and prompt reporting of any privacy or security incident. These processes include:

1) RAC or Partnership's Privacy Officer shall notify DHCS within 24 hours of the date of discovery by any Partnership employee, officer, or agent. A privacy incident shall be treated as discovered as of the first day on which the incident is known, or by exercising reasonable diligence would have been known, to any person (other than the person who caused the incident) who is an employee, officer or agent of Partnership.

2) Within 24 hours of the date of discovery, Partnership will notify the DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer via secure email, fax, or telephone, whichever is the most appropriate means of notification, of a privacy incident, privacy breach, or security incident.

3) Within 72 hours of the date of discovery and following the initial report, Partnership will conduct an investigation of all reported incidents and provide an updated report to DHCS by submitting a "DHCS Privacy Incident Report", which shall include all necessary information known at the time of submission. This form is to be completed via the Department of Health Care Services Privacy Incident Reporting Portal.

4) Within (10) working days of the date of discovery of the incident, Partnership will submit,

an updated Privacy Incident Report, via the Department of Health Care Services Privacy Incident Reporting Portal.

4. Internal Investigations of Incidents or Breaches
   a. RAC, upon receipt of a privacy referral, shall immediately begin an investigation of the issue(s) contained in the report.
      1) Per 45 CFR §160.306, reports made after 180 days from the date of the complainant knew or should have known that the act or omission occurred may not be accepted by Partnership, unless good cause is demonstrated.
      2) The Privacy Officer or Compliance Officer, with input as necessary from the Compliance Committee, may decide what constitutes good cause.
   b. Partnership's Privacy Officer, or designee, shall be responsible for the management of the breach investigation, completion of the risk assessment, and may follow up with the individual completing the initial Incident Reporting Form, as necessary to clarify the initial report, to obtain additional information, or take prompt corrective action to mitigate any risks or damages involved with the incident and to protect the operating environment. Follow up requests may be sent from EthicsPoint directly, or via email.
   c. Where a privacy incident results from a member grievance or complaint, Partnership Privacy Officer or designee, will coordinate with the assigned Grievance staff to inform the member(s) of the outcome of the privacy investigation of their complaint, after consultation with the applicable regulatory oversight agency.
5. Risk Assessment
   a. Per 45 CFR §164.414, Partnership retains the burden of proof to demonstrate that all notifications are provided or that an impermissible use or disclosure does not constitute a breach. In order to determine whether member notification is necessary, RAC must conduct an objective risk assessment based on the details gathered during the course of the investigation to determine whether the protected information has been compromised.
   b. To determine if there is a low possibility that the protected information has been compromised, the following factors must be considered:
      1) The nature and extent of the protected information involved, including the types of identifiers and the likelihood of re-identification;
      2) The unauthorized party who used the protected information or to whom the disclosure was made;
      3) The extent in which Partnership was notified of the exposed protected information, whether it was immediate, a few days after, or never; and
      4) The extent to which the risk to the protected information has been mitigated.
   c. If, through an objective risk assessment, Partnership cannot reasonably demonstrate that there is a low probability that the protected information has been compromised, breach notification to affected members is necessary.
6. Breach Notification
   a. Within 60 calendar days and without reasonable delay, Partnership shall notify individuals of a confirmed privacy breach or unauthorized use or disclosure when notification is required under state or federal law. (Pursuant to §164.404(a) and (b))
   b. Privacy breaches involving less than 500 members: within 60 calendar days of the end of each calendar year, Partnership shall report privacy breaches involving less than 500 members to the Office of Civil Rights.
   c. Privacy breaches involving more than 500 members: Partnership shall notify the California Office of Civil Rights and Secretary of State immediately when a privacy breach involves more than 500 members
   d. Pursuant to 45 CFR §164.406, for breaches involving more than 500 members: Partnership well

notify prominent media outlets serving the State or jurisdiction.

7. Law Enforcement Delay of Breach Notification
   a. Pursuant to 45 C.F.R. § 164.412, if a law enforcement official states that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, Partnership shall:
      1) If statement is in writing and specifies the time for which a delay is required, delay the notification, notice, or posting for the time period specified by the official; or
      2) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay notification, notice, or posting temporarily and no longer than 30 days unless a written statement is received during that time.
8. Content of Notice
   a. The notice shall be written in plain language using the templates provided by DHCS in the State of California Department of Technology Office of Information Security, SIMM 5340-C and will include the following information (Pursuant to 45 C.F.R. § 164.404(c)).
      1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
      2) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
      3) Any steps the individual should take to protect themselves from potential harm resulting from the breach.
      4) A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
      5) Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.
   b. Notices to members require review and approval prior to being mailed to the member.
   c. Notices will be sent by first-class mail to the member at the last known address, unless an alternative method is request by the member or the notice is unable to be mailed in which the Privacy Officer may approve a substitute form of notice to reach the member.
9. Retaliation/Waiver
   a. Partnership workforce may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against a member for exercising their privacy rights. Members shall not be required to waive their privacy rights as a condition of the provision of treatment, payment, or eligibility for benefits.

VII. REFERENCES:

A. 45 CFR §160 and 164 et. seq.
B. HITECH Act; Breach Notification for Unsecured Protected Health Information Interim Rule
C. California Civil Code §1798.29 and §1798.82
D. California Civil Code §56 et. seq.
E. Welfare & Institutions Code 5328 and the CA Confidentiality of Medical Information Act
F. California State Breach Notification Law (AB 1298)
G. DHCS Medi-Cal Contract 23-30236, Exhibit G, Business Associate Addendum
H. Instructions for Submitting Notice of a Breach to the Secretary (45 CFR §164.408) (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html)

VIII. DISTRIBUTION:

A. PowerDMS

B. PHC 4 Me
C. Directors
D. Provider Manual

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE:
Privacy Officer

X. REVISION DATES:
Medi-Cal
06/18/10, 12/06/11, 12/04/12, 03/26/12, 09/01/15, 09/07/16, 02/22/2018, 03/07/2019, 02/20/2020, 02/18/2021, 12/02/2021, 11/17/2022, 11/16/2023, 11/21/2024

PREVIOUSLY APPLIED TO:
PartnershipAdvantage:
CMP-18 - 05/01/09 to 01/01/2015
Healthy Families:
CMP-18 - 10/01/2010 to 03/01/2013
Healthy Kids
CMP-18 – 05/01/09 to 12/01/16