**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<br>☒ Internal Policy</td></tr>
<tr><td colspan="2">Original Date: 05/01/2009</td><td colspan="4">Next Review Date: 09/03/2027<br>Last Review Date: 09/03/2026</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: 09/03/2026</td></tr>
</table>

## I. RELATED POLICIES:

A. CMP-10- Confidentiality
B. CMP-13 Permitted Use, Disclosure, and Minimum Necessary Use of Member Information
C. CMP-23 External PHI Release Control
D. CMP-24 Physical and Administrative Safeguards
E. CMP-26 Verification of Caller Identity and Release of Information
F. CMP-41 Wellness and Recovery Program Records

## II. IMPACTED DEPTS.:

All.

## III. DEFINITIONS:

B. 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. (Pursuant to 45 CFR § 164.404(a)(2).) Disability Status data, including function and identity: refers to member's self-identified disability status, which per NCQA definition includes, to the extent possible, all individuals who may face barriers to accessing appropriate, timely health care services, and who may experience disparities in health outcomes.
C. Gender Identity: per National Committee for Quality Assurance (NCQA) health equity accreditation standards, means an individual's innermost concept of self and experience of gender, which may be different from the sex assigned at birth.
(Pursuant to 45 CFR § 164.404(a)(2).)
D. Privacy Breach: A privacy breach means, unless expressly excluded under 45 C.F.R. § 164.402, the acquisition, access, use, or disclosure of PHI in a manner not permitted under Subpart E of 45 C.F.R. Part 164 which compromises the security or privacy of the PHI and as more particularly defined under 45 C.F.R. § 164.402.
E. Privacy Incident Report: A report which contains details of a privacy issue involving Partnership members and their PHI.
F. 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.
G. Protected Health Information: For the purposes of this policy, Protected Health Information (PHI) is any information that can be used to individually identify a Partnership member and explicitly related to the individuals past, present, or future healthcare. PHI data points may include but are not limited to:

i. Health status data: past, present, or future physical or mental conditions. which includes but is not limited to disability Status (including function and identity), race/ethnicity and language (REAL), sexual orientation, and gender identity
ii. Healthcare payment data: past, present, or future payment details for healthcare services
iii. Healthcare services data: the provision of care and treatments given to a person such as medical record number or health plan beneficiary number in context of diagnosis information, photographic images related to condition or treatment, medical history, and/or prescription information.

H. Personally Identifiable Information (PII): Consistent with the Information Practices Act (IPA) at California Civil Code section 1798.3(a) personally identifiable information (PII) means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to:
   i. Individual's name
   ii. Social security number
   iii. Physical description
   iv. Home address
   v. Email address
   vi. Telephone number
   vii. Education
   viii. Licensing records
   ix. Any other unique identifying number, characteristic, or code

,

I. Substance Use Disorder (SUD) Information/Records: Records protected under 42 CFR Part 2 relating to the diagnosis, treatment, or referral of treatment of substance use disorders. Unauthorized acquisition, use, access, or disclosure of SUD records under 42 CFR Part 2 is considered a privacy incident or breach.
J. 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.
K. 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.
L. Race/ethnicity and language (REAL) data: refers to member's self-identified and reported REAL information, which may be collected by Partnership directly as self-reported from the individual or reported via state eligibility and enrollment data
M. Sexual orientation: per NCQA health equity accreditation standards, means an inherent or immutable and enduring emotional, romantic or sexual attraction or nonattraction to individuals of the same and/or other genders

## I. ATTACHMENTS:

N/A

## II. 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.

**III. POLICY / PROCEDURE:**

A. Policy:

1. As a Covered Entity, Partnership is beholden to The Privacy Rule issued by the U.S. Department of Health and Human Services that mandates protection of 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;
    d. and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.
2. Partnership is required to implement processes to support the identification and prompt reporting of incidents or breaches involving protected health information (PHI). (45 CFR § 164.402.)
3. 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.
4. In compliance with DHCS Medi-Cal Contract 23-30236, Exhibit G, Business Associate Addendum 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. (45 CFR § 164.308(a)(5) (Security awareness training requirement); 45 CFR 164.530(b) (1) (Privacy training requirement).)
5. Partnership Workforce shall follow standards required by state and federal law when handling PHI. Prior to disclosure of PHI, Partnership Workforce must verify the identity of the requester. PHI shall only be released to authorized individuals or entities as permitted by law. Unauthorized use or disclosure will be treated as a privacy violation and subject to disciplinary action.
6. Partnership Workforce shall access only the minimum necessary PHI needed to perform job duties. PHI must not be transmitted via unencrypted email, SMS, or personal devices unless approved and secured.
7. Partnership Workforce shall not take it upon themselves to determine at the point of discovery whether an incident is deemed a breach.
8. 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 identification of a potential or actual privacy incident, 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. 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 report the incident immediately upon identification. The completed form should contain all information requested known to the individual reporting the incident and shall include the date of awareness 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.
   b. Incidents involving SUD Records protected under 42 CFR Part 2 are subject to the same breach notification requirements and civil enforcement authorities applicable under HIPAA. Such incidents shall be investigated, risk assessed, documented, and reported in accordance with applicable HIPAA Privacy, Security, and Breach Notification Rule requirements.

3. Partnership's Regulatory Reporting Requirements
   a. Pursuant to DHCS Contract 23-30236, Exhibit G, Provision, Partnership maintains processes to support the identification and prompt reporting of any privacy or security incident. These processes include:
      1) Upon notification of a suspected or actual privacy incident, RAC or Partnership's Privacy Officer shall notify DHCS within 24 hours. 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 , RAC 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 (10) working days of notification 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 (b)(3), reports made after 180 days from the date of when 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 (b), 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. as defined in 45 CFR § 164.402. In order to determine whether member notification is necessary, RAC must conduct an objective risk assessment based on the details gathered during the investigation to determine whether the protected information has been compromised.
   b. The break risk assessment requirements described in this policy apply equally to PHI and SUD records protected under 42 CFR Part 2.
   c. 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.
   d. 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. per 45 CFR § 164.402(2):

6. Breach Notification

   a. Within 60 calendar days unless a shorter timeframe is required by DHCS and without reasonable delay, Partnership shall notify individuals of a HIPAA privacy breach or unauthorized use or disclosure when notification is required under federal law. (Pursuant to §164.404(a) and (b)); DHCS Contract, Exhibit G, Section 18.4). For breaches involving California residents' personal information as defined under Civil Code §1798.82, notification must be made within 30 calendar days of discovery or receipt of notice of the breach, unless delayed to accommodate the legitimate needs of law enforcement or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system (in accordance with SB 446).
   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 U.S. Department of Health and Human Services, Office of Civil Rights. (Pursuant to §164.408(c).) Partnership must also make a timely report to DHCS and any other California

agency as required under applicable law. (DHCS Contract, Exhibit G, Section 18.1.)

c. Privacy breaches involving more than 500 members: Partnership shall notify the HHS Secretary and OCR immediately when a privacy breach involves more than 500 members. (Pursuant to § 164.408(b).)
d. Privacy breaches involving more than 500 members: Partnership shall submit a sample copy of the consumer notification to the California Attorney General within 15 calendar days after notifying affected individuals, in accordance with Cal. Civ. Code §1798.82(f). Partnership must also make a timely report to
DHCS, and any other California agency as required under applicable law. (Cal. Civ. Code § 1798.29(e); DHCS Contract, Exhibit G, Section 18.1.)
e. Pursuant to 45 CFR §164.406, for breaches involving more than 500 members: Partnership well notify prominent media outlets serving the State or jurisdiction.
f. Covered entities that fully comply with HITECH 13402(f) requirements are considered compliant with Cal. Civ. Code §1798.82 notice requirements.

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 must be titled "Notice of Data Breach", at least 10-point font, and 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.
      6) Use of the following headings: (a) What Happened?, (b) What Information Was Involved?, (c) What We Are Doing, (d) What You Can Do, (e) For More Information.
   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.
   d. If Partnership is the source of the breach and the information of the affected individual involved includes their SSN, driver's license numbers, financial account information, or other sensitive

personal information, Partnership shall provide affected individuals with identity theft prevention and mitigation services for a minimum of12 months, including enrollment and access instructions.

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.

## IV. 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)

## V. DISTRIBUTION:

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

## VI. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE:

Privacy Officer

## VII. 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, 11/04/2025, 02/10/2026, 09/03/2026

**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
Administration
ADM-22 12/02/16 to 2/10/2026

| | | | |
|---|---|---|---|
| **Policy/Procedure Number: CMP-18** (Formerly ADM-20) | | | **Lead Department: Administration** |
| **Policy/Procedure Title:** Reporting Privacy Incidents and Breach Notification | | | ☒**External Policy**<br>☒**Internal Policy** |
| **Original Date:** 05/01/2009 | | **Next Review Date: 09/03/2027**<br>**Last Review Date: 09/03/2026** | |
| **Applies to:** | ☒ **Medi-Cal** | ☐ **Healthy Kids** | ☒ **Employees** |