MEETING AGENDA

Meeting: Governance / Compliance Committee

Date: February 22, 2024 **Time**: 2:00PM-3:00PM

Location: PHC Offices:
1. PHC's Southeast Office located at 4665 Business Center Dr, Fairfield, CA
2. PHC's Northwest Office located at 1036 Fifth Street, Eureka, CA
3. PHC's Northeast Office located at 2525 Airpark Drive, Redding, CA
4. PHC's Southwest Office located at 495 Tesconi Circle, Santa Rosa, CA
5. 1003 Gravenstein Hwy North, Sebastopol, 95472

Members: Lewis Broschard, Cathryn Couch, Alicia Hardy, Lance LeClair, Wendy Longwell, Tory Starr, Kim Tangermann

Staff: Sonja Bjork (CEO), Danielle Ogren (Director of Regulatory Affairs), Amy Turnipseed (Chief Strategy and Government Affairs Officer), Wendi Davis (COO)

Optional: Dr. Moore (CMO), Kirt Kemp (CIO)

Topic	Notes
1) Call to Order	
2) ACTION: Approval of November 29 Minutes *Time: 5 minutes* *Speaker: Chair* *Pages: 3-4*	
3) INFORMATION: Compliance/Privacy Officer Update *Time: 15 minutes* *Speaker: Danielle Ogren*	
4) INFORMATION: Security Officer Update/ Security Audit Outcome and Activities *Time: 15 minutes* *Speaker: Kirt Kemp*	
5) ACTION: Review and Approve Compliance Program Dashboard, Policies, All Plan Letters (see separate packet) *Time: 25 minutes*	

Speaker: Amy Turnipseed / Danielle Ogren *Pages: 5-109*	

MEETING MINUTES

Meeting: Governance / Compliance Committee

Date: November 29, 2023

Time: 10:00AM-11:00AM

Location: PHC Offices:
1. PHC's Southeast Office located at 4665 Business Center Dr, Fairfield, CA (HR Training Room)
2. PHC's Northwest Office located at 1036 Fifth Street, Eureka, CA
3. PHC's Northeast Office located at 2525 Airpark Drive, Redding, CA
4. PHC's Southwest Office located at 495 Tesconi Circle, Santa Rosa, CA

Coordinator: Jessica Cifolelli

Members Present: Cathryn Couch, Alicia Hardy, Wendy Longwell,

Members Excused: Kim Tangermann, Dr. Broschard, Tory Starr, Lance LeClair

Staff Present: Sonja Bjork (Deputy CEO), Amy Turnipseed (Chief Strategy Officer), Wendi West (Deputy COO), Danielle Ogren (Director of Regulatory Affairs and Program Development) Ashlyn Scott (Board Clerk) Jessica Cifolelli (Executive Assistant)

Topic	Notes
1) Objective of Meeting *Speaker: Sonja Bjork*	Chair, Cathryn Couch, called the meeting to order at 10:05 am a quorum was not met. Ms. Bjork stated that the purpose of the meeting will be to discuss Partnership HealthPlan's Compliance updates and updated document/report approval process.
2) ACTION: Approval of August 17, 2023 Minutes *Speaker: Chair*	**The committee approved the August 17, 2023 minutes as presented.** *Cathryn Couch motioned and Alicia Hardy seconded. Motion passed.*
3) INFORMATION: County Ordinance Update *Speaker: Amy Turnipseed*	Ms. Turnipseed shared that meetings have been taking place with the 24 counties to discuss the new ordinance template. As of today 19 of the 24 counties meeting have taken place with 5 remaining to be scheduled.

4) INFORMATION: 2024 Board DEI Metrics and Report *Speaker: Ashlyn Scott*	Ms. Scott shared with the committee that NCQA is requiring Diversity, Equity, and Inclusion information by March 2024. She will be reaching out to board members for personal information in March. This will be done annually. The report will be shared with the Governance and Compliance Committee. PHC's consultant recommended that Diversity, Equity, and Inclusion be included in the bylaws. The board has an obligation to ensure that the health needs of all populations within that community are equitably served. *Ms. Bjork noted that there will be a different reception based on the county.*
5) ACTION: Approve the revised Committee Charter *Speaker: Amy Turnipseed*	Ms. Turnipseed shared with the committee that Danielle Ogren has taken the position of Compliance and Privacy Officer. Technical changes have been made to the Compliance Committee charter. Ms. Turnipseed asked committee members to review the Compliance Committee charter carefully and to note if further changes needed to be made before approval.
6) ACTION: Review and Approve Compliance Program Dashboard, Compliance Plan, Audit Work Plan *Speaker: Amy Turnipseed/Danielle Ogren*	Ms. Ogren shared the following information regarding the Compliance Plan with the committee. RAC, through the risk assessment, surveyed operational leadership to identify potential risks to the plan and specifically to the Compliance Program in 2024. As a result, the top five risk priorities include: DHCS 2024 Contract Restatement, Cyber Security, New Claims System Implementation, Medi-Cal Delivery System Reform/California Advancing and Innovating Medi-Cal, and Geographic Expansion – County Plan Model Changes. The committee reviewed the Q3 Compliance Dashboard. The dashboard includes important metrics used to ensure we are reporting FWA and privacy breaches. As we go forward, this will evolve and change. Ms. Turnipseed shared that going forward the consent agenda from the Compliance Committee will be reviewed by the Governance and Compliance Committee then report to the Board.

February 2024 Governance/ Compliance Committee
Policy Summary – Discussion

Consent Agenda		
Policies and Procedures		
Item	Last Approved Date	Summary of Item
CPM 03 Compliance Approval Process	2/15/2024	Technical updates include: - Next review date - Last review date - Approval Signature- updated to show Sonja Bjork as CEO - Section VI. Policy and Procedure - Reference- update to DHCS contract reference - Revision date
CMP 07 False Claims Act	2/15/2024	Technical updates include: - Next review date - Last review date - Approval Signature- updated to show Sonja Bjork as CEO - Approval date - Updated related policy number to FIN-405 - Section VI.A.1- update to DHCS contract reference - Reference- update to DHCS contract reference - Revision date
CPM 09 Investigating And Reporting FWA	2/15/2024	Technical updates include: - DHCS contract reference updated throughout the policy. - Next review date - Last review date - Approval Signature- updated to show Sonja Bjork as CEO - Approval date - Updated related policy number to FIN-405 - Definition of waste. - Attachments to include Fraud Prevention Program - Section VI.A.1- update to DHCS contract reference and removed language that was not relevant to CMP-09 - Section VI.B.4(b)- update reporting requirements for the completed investigations. - Revision date

CMP 20 Brown Act Compliance	2/15/2024	Section VI. Policy/Procedure Subsection A.4. Teleconferencing date has been extended to 1/1/2026 under specific circumstances per AB 2449. Attachment A Committee list has been updated
CMP 21 Conflict of Interest	2/15/2024	Technical updates include: - Next review date - Last review date - Approval Signature- updated to show Sonja Bjork as CEO - I. Related Policies removes of CMP 17 Glossary of Terms - Revision date
CMP39 Regulatory Change Management	2/15/2024	Updated section VI (A) (3) to describe department's responsibility to notify RAC regarding any issues meeting compliance deadlines (4) to make clear the responsibility of departments to work on guidance outside of the RCM meeting Updated section VI (B) (2) to address department responsibilities regarding making updates to RCM workgroup (4) department responsibility for submitting regulatory guidance deliverables

All Plan Letters (APL)

Item	Release Date	Eff.	Summary of Item
APL 23-031 Medi-Cal Managed Care Plan Implementation of Primary Care Provider Assignment for the Age 26-49 Adult Expansion Transition	12/20/2023	Upon release	Purpose/policy: Guidance on the Age 26-49 Adult Expansion to ensure individuals transitioning from restricted scope Medi-Cal or are otherwise uninsured to full-scope Medi-Cal maintain their existing Primary Care Provider (PCP) assignments to the maximum extent possible to minimize disruptions in services. Action required: • provide policies and procedures to the Regulatory Guidance inbox by March 12, 2024.

APL 23-032 Enhance Care Management Requirements	12/22/2023	Upon release	Purpose/policy: Provide guidance to all Medi-Cal managed care plans (MCPs) regarding the provision of the Enhanced Care Management (ECM) benefit. Action required: • provide policies and procedures to the Regulatory Guidance inbox by March 14, 2024.
APL 23-034 California Children's Services Whole Child Model Program	12/27/2023	Upon release	Purpose/policy: Provide guidance to MCPs participating in the California Children's Services (CCS) Whole Child Model (WCM) Program. [*Supersedes APL 21-005*] Action required: • Within 90 days from the release of the APL, PHC must submit an attestation of no impact or a revised policy to address APL requirements. Please submit P&P's to Regulatory Guidance by March 19, 2024.
APL 23-035 Student Behavioral Health Incentive Program	12/28/2023	Upon release	Purpose/policy: Provide Medi-Cal managed care plans (MCPs) with guidance on the incentive payments provided by the Student Behavioral Health Incentive Program (SBHIP). SBHIP is a part of California's Children and Youth Behavioral Health Initiative (CYBHI) and is being implemented by the Department of Health Care Services (DHCS) Action required: • Please provide a P&P or a completed internal checklist (if no P&P updates are needed) to the Regulatory Guidance inbox by March 20, 2024.

APL 24-001 Street Medicine Provider: Definitions and Participation in Managed Care	1/12/2024	Upon release	Purpose/policy: Provide guidance to Medi-Cal managed care plans (MCPs) on opportunities to utilize street medicine providers to address clinical and non-clinical needs of their Medi-Cal Members experiencing unsheltered homelessness. [*Supersedes APL 22-023]* Action required: • Please provide a P&P or a completed internal checklist (if no P&P updates are needed) to Regulatory Guidance by April 4, 2024.
APL 24-002 Medi-Cal Managed Care Plan Responsibilities for Indian Health Care Providers and American Indian Members	2/8/2024	Upon release	Purpose/policy: Summarize and clarify existing federal and state protections and alternative health coverage options for American Indian Members enrolled in Medi-Cal managed care plans (MCPs). Additionally, this APL consolidates various MCP requirements pertaining to protections for Indian Health Care Providers (IHCPs), including requirements related to contracting with IHCPs and reimbursing claims from IHCPs in a timely and expeditious manner. This APL also provides guidance regarding MCP tribal liaison requirements and expectations in relation to their role and responsibilities. [*Supersedes APL 09-009]*

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY / PROCEDURE

<table>
<tr><td colspan="3">Policy/Procedure Number: CMP-07</td><td colspan="3">Lead Department: Administration</td></tr>
<tr><td colspan="3">Policy/Procedure Title: False Claims Act</td><td colspan="3">☒ External Policy
☒ Internal Policy</td></tr>
<tr><td colspan="2">Original Date: 07/01/2007</td><td colspan="4">Next Review Date: ~~05/18/2024~~ 2/15/2024
Last Review Date: ~~05/18/2023~~ 2/15/2024</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: ~~Elizabeth Gibboney~~ Sonja Bjork, CEO</td><td colspan="3">Approval Date: ~~05/18/2023~~ 2/15/2024</td></tr>
</table>

I. RELATED POLICIES:

A. ADM-47 Administrative and Financial Sanctions
B. CMP-09 Investigating & Reporting Fraud, Waste and Abuse
C. CMP-27 Non-Intimidation & Non-Retaliation
D. FIN~~-700~~-405 Treatment of Recoveries of Overpayments to Providers

II. IMPACTED DEPTS.:

All

III. DEFINITIONS:

A. Knowingly: means that a person, with respect to information: (a) has actual knowledge of the information; (b) acts in deliberate ignorance of the truth or falsity of the information; or (c) acts in reckless disregard of the truth or falsity of the information. Proof of specific intent to defraud is not required.
B. Overpayment: means any payment made to a participating provider by PHC to which the provider is not entitled to under Title XIX of the Social Security Act.
C. PHC 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 PHC Board of Commissioners employed by or acting on the behalf of PHC.

IV. ATTACHMENTS:

N/A

V. PURPOSE:

The purpose of this policy is to inform PHC's workforce members and affiliates about certain federal and state false claims and whistleblower laws in compliance with the requirements of Section 6032 of the Deficit Reduction Act of 2005 (DRA), 42 USC Section 1396a(a)(68) and California Government Code §12650.

VI. POLICY / PROCEDURE:

A. Policy

1. In compliance with Department of Healthcare Services (DHCS) Contract ~~08-85215~~23-30236, Exhibit ~~E~~A, Attachment ~~2~~III, Provision 1.3.7(A)~~27(C)(6)~~, as a Managed Medi-Cal Plan that makes or receives

annual payments under this contract of at least five million dollars ($5,000,000), PHC must ensure that its workforce members are provided with detailed information about the False Claims Act and other federal and State laws described in Section 1902(a)(68) of the Act, including information about rights of employees to be protected as whistleblowers.

2. State Law
   a. The State of California has established the California False Claims Act as found in California Government Code §12650. The State of California Department of Justice False Claims Unit under the direction of the Attorney General works to protect the state against fraud and other financial misconduct through the enforcement of the California False Claims Act.
      i. This permits the Attorney General to bring civil law enforcement action and civil penalties against any person who knowingly makes or uses a false statement or document to either obtain money or property from the State or avoid paying or transmitting money or property to the State.
      ii. Violations of the Act involving the Medi-Cal program are investigated and prosecuted by the Attorney General's Bureau of Medi-Cal Fraud & Elder Abuse.

3. Federal False Claims Act (FCA)
   a. The Federal False Claims Act as contained in 31 U.S.C. § 3729-3733 is designed to both prevent and protect the U.S. Government from fraud. The FCA contains provisions including, but not limited to, prohibitions, enforcement, and financial incentive for individuals, known as relators or "whistleblowers", retaliation and penalties.

4. Prohibitions
   a. The FCA prohibits, among other things:
      i. Knowingly presenting or causing to be presented to the federal government a false or fraudulent claim for payment or approval;
      ii. Knowingly making or using, or causing to be made or used, a false record or statement in order to have a false or fraudulent claim paid or approved by the government.
      iii. Conspiring to defraud the government by getting a false or fraudulent claim allowed or paid; and
      iv. Knowingly making or using, or causing to ~~me~~ be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay or repay an overpayment

5. Enforcement
   a. The Attorney General may bring civil law enforcement action to recover treble damages and civil penalties against any person who knowingly makes or uses a false statement or document to either obtain money or property from the government or avoid paying or transmitting money or property to the government. The False Claims Unit of the Corporate Fraud Section investigates alleged violations of the Act based upon referrals from state, federal and local agencies, tips from members of the public and qui tam complaints, otherwise known as whistleblower complaints.

6. Federal Law Whistleblower Provisions
   a. The FCA permits a private person with actual knowledge of false claims activity to file a civil lawsuit on behalf of the federal government. These are known as "qui tam" or "whistleblower" provisions of the FCA and contain detailed procedures for how to file such lawsuits. The purpose of a qui tam suit is to recover the funds paid by the federal government as a result of false claims.

7. Federal Law Protections Against Retaliation
   a. The FCA also protects employees from retaliation or discrimination in terms and conditions of their employment based on lawful acts of the employee done in furtherance of an action under the FCA. This applies to any employee who is discharged, demoted, suspended, threatened, harassed, or discriminated against in his or her employment as a result of the employee's lawful acts in furtherance of a FCA.

8. Penalties
   a. Penalties for violating the FCA include up to three times the amount of damage sustained by the federal government, civil monetary penalties, and/or exclusion from federally funded programs. Federal law also contains criminal and administrative sanctions for false claims and statements that may be applicable to identified instances of health care fraud, waste and abuse. Note: Medi-Cal is both a federal and state funded program governed by the California Department of Health Care Services (DHCS). DHCS sanctions shall be imposed pursuant to DHCS All Plan Letter (APL) 18-003 and assessed for pass through to DHCS subcontractors, delegates, and/or network providers consistent with PHC policy and procedure ADM 47 Administrative and Financial Sanctions

9. PHC Notification regarding the False Claims Act Requirements:
   a. PHC ensures workforce members and affiliate awareness of federal and state False Claims Act provisions and whistleblower protections by:
      i. Making this policy available both internally and externally for review and when necessary, reference.
      ii. Facilitating PHC workforce member compliance training at the time of onboarding and annually thereafter to include FCA requirements
      iii. Making available the applicable policies for monitoring claims and authorization for services and supplies to serve as the basic mechanism for detecting potential FCA violations.

B. Procedure

1. Reporting potential or actual False Claims Violations
   a. In accordance with PHC policy and procedure CMP-09 Investigating & Reporting Fraud, Waste, and Abuse, if a PHC workforce member or affiliate suspects a potential or actual violation of any of the federal or state FCA requirements, a referral to RAC shall be made by:
      i. Internal workforce: Completing the EthicsPoint RAC Intake Form (accessible through PHC's intranet, PHC4Me, or
      ii. External parties: Completing a referral using PHC's Incident Reporting form (available on PHC'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 PHC management, RAC, or the PHC Compliance Officer.

2. Investigation of potential or actual False Claim Act Violations
   a. Upon receiving a report of potential or suspected FWA, PHC's Compliance Officer, or designee will review the referral and conduct a preliminary investigation of the case. During the preliminary investigation, RAC may, when appropriate, review the case in collaboration with other PHC units or executive leadership.
      i. PHC shall also notify and consult with state and federal regulatory agencies

including, but not limited to, DHCS, Centers for Medicare and Medicaid Services, Office of Inspector General, and/or the Attorney General, as necessary to conduct a thorough review of all claims and/or requests for authorization of services and/or supplies by the entity under review.

b. As such and consistent with the 2024 DHCS Medi-Cal contract, Exhibit A, Attachment III, Provision 1.3.7 *Federal False Claims Act Compliance and Support*, PHC shall fully cooperate in any investigation or prosecution conducted by the Office of the Attorney General, Division of Medi-Cal Fraud and Elder Abuse (DMFEA) and the US DOJ. Cooperation may include provision of information and records upon request, staff participation in interviews, consultation, grand jury proceedings, pre-trial conference, depositions, and hearings at DHCS.

3. Violations under the False Claims Act
   a. If PHC or any of the involved regulatory agencies concludes that a contracted entity under review is in a violation of the FCA , PHC shall provide written notification to the entity describing the violation in detail and shall include:
      i. Instructions to immediately cease and desist from further engaging in the practice;
      ii. Detailed findings of violation with the False Claims Act;
      iii. Reference to the applicable statutory, regulatory, contractual, PHC policy and procedures, or other requirements that are the basis of the findings;
      iv. Corrective action that may include the imposition of administrative or financial sanctions or penalties, up to the revocation of the contract;
      v. Timeframes by which the organization or individual shall be required to achieve compliance, as applicable; and
      vi. Indication that the activities cited in the notification may serve as a basis for referral to the appropriate regulatory authorities
   b. In accordance with 42 CFR 438.608(8)(d) and processes established under PHC policy and procedure FIN-~~700~~-405, PHC shall promptly report to DHCS all overpayments identified or recovered due to potential fraud and shall pursue recoveries of any overpayments related to identified FWA activities.
   c. In the case that a violation of the False Claims Act is founded, PHC may, in addition to any recoupment of overpayment or civil penalties accessed by regulatory agencies, impose administrative or financial sanctions against the entity in violation and in accordance with PHC policy and procedure ADM-47 Administrative and Financial Sanctions.

4. Qui Tam Relators
   a. PHC and its workforce members shall fully cooperate in actions brought by qui tam relators pursuant to 31 U.S.C. § 3730(b), to the extent such actions involve services rendered to PHC members.
   b. PHC's subcontractors and delegates are specifically directed to comply with the prohibition on retaliating against qui tam relators. 31 U.S.C. § 3730(h). To the extent PHC workforce members become aware of any retaliatory action toward a qui tam relator employed by a PHC provider or supplier, reasonable efforts shall be undertaken to inform the employer of its statutory obligation to refrain from such actions.

VII. REFERENCES:

A. Federal Deficit Reduction Act of 2005

B. U.S. Code: Title 31 § 3729-3733
C. 42 CFR §438.608
D. State of California Department of Justice False Claims Unit - https://oag.ca.gov/cfs/falseclaims
~~E. DHCS Contract 08-85215, Exhibit E, Attachment 2, Provision 27 (C)(6),~~
~~F.~~E. 2024 DHCS Medi-Cal contract, Exhibit A, Attachment III, Provision 1.3.7 *Federal False Claims Act Compliance and Support*,
A. DHCS All Plan Letter (APL) 18-003

VIII. DISTRIBUTION:

A. California Department of Health Care Services
B. Provider Manual
C. PowerDMS
D. Directors

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE:

N/A

X. REVISION DATES:

Medi-Cal
03/02/2010, 12/06/2011, 12/04/2012, 03/26/2013, 12/01/2015, 12/06/2016, 05/17/2017, 05/24/2018, 05/16/2019, 02/20/2020, 02/18/2021, 02/17/2022, 02/16/2023, 05/18/2023, 2/15/2024

PREVIOUSLY APPLIED TO:

PartnershipAdvantage:
CMP-07 - 07/01/2007 to 01/01/2015
Healthy Families:
CMP-07 - 07/01/2007 to 03/01/2013
Healthy Kids
CMP-07 – 07/01/2007 to 12/01/2016

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY / PROCEDURE

Policy/Procedure Number: CMP-09			**Lead Department: Administration**	
Policy/Procedure Title: Investigating & Reporting Fraud, Waste and Abuse			☒ **External Policy** ☒ **Internal Policy**	
Original Date: 03/02/2010		**Next Review Date:** ~~02/16/2024~~ 02/15/2025 **Last Review Date:** ~~02/16/2023~~ 02/15/2024		
Applies to:	☒ **Medi-Cal**	☐ **Healthy Kids**	☒ **Employees**	
Reviewing Entities:	☐ **IQI**	☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**	☐ **EXECUTIVE**	☐ **COMPLIANCE**	☐ **DEPARTMENT**
Approving Entities:	☐ **BOARD**	☒ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☐ **CEO** ☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: ~~*Liz Gibbons*~~ *Sonja Bjork, CEO*			**Approval Date:** ~~02/16/2023~~ 02/15/2024	

I. RELATED POLICIES:

A. CMP-06 Compliance Issues and Complaints
B. CMP-07 False Claims Act
C. CMP-10 Confidentiality
D. CMP-18 Reporting Privacy Incidents and Breach Notifications
E. CMP-27 Non-intimidation & Non-retaliation
F. CMP-28 Compliance Training Program Requirements
G. CMP-30 Records Retention and Access Requirements
H. FIN~~-700~~-405 Treatment of Recoveries of Overpayments to Providers
I. MPRP4036 Pharmacy Benefit Manager (PBM) Claims and Business Records Auditing
J. MPRP4062 Drug Wastage Payments

II. IMPACTED DEPTS.:

All

III. DEFINITIONS:

A. Fraud: means an intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to him or herself or some other person. It includes any act that constitutes fraud under applicable Federal or State law. (42 CFR 452.2: W. & I. Code Section 14043.1(i).
B. Waste: means the overutilization or inappropriate utilization of services and misuse of resources, ~~and typically is not a criminal or intentional act, as stated in CMS' Fraud, Waste and Abuse Toolkit.~~per DHCS Medi-Cal contract.
C. Abuse: means provider practices that are inconsistent with sound fiscal, business, or medical practices, and result in an unnecessary cost to the Medicaid program, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. It also includes recipient practices that result in unnecessary cost to the Medicaid program (42 CFR 455.2 and as further defined in W. & I. Code Section 14043.1(a).)
D. PHC 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 PHC Board of Commissioners employed by or acting on the behalf of PHC.

IV. ATTACHMENTS:

A. Fraud Prevention Program

Policy/Procedure Number: CMP-09		Lead Department: Administration	
Policy/Procedure Title: Investigating and Reporting Fraud, Waste and Abuse		☒External Policy ☒Internal Policy	
Original Date: 03/02/2010		**Next Review Date:** ~~02/16/2024~~ 02/15/2025 **Last Review Date:** ~~02/16/2023~~ 02/15/2024	
Applies to:	☒ Medi-Cal	☐ Healthy Kids	☒ Employees

~~A.~~B. FWA Investigations and Overpayment Recovery Workflow

V. PURPOSE:

This policy outlines Partnership HealthPlan of California's (PHC) process to detect, prevent, investigate, and report potential or actual cases of fraud, waste or abuse (FWA).

VI. POLICY / PROCEDURE:

A. Policy

A. PHC Responsibilities Under the Contract with the Department of Health Care Services (DHCS)

1. In compliance with DHCS Contract ~~08-85215~~23-30236, Exhibit ~~E~~A, Attachment ~~2~~III, PHC shall meet the requirements set forth in 42 CFR § 438.608 by establishing administrative and management arrangements or procedures, ~~as well as~~ mandatory compliance plan, fraud prevention program, and designation of a fraud prevention officer, which are designed to ~~guard~~ prevent and detect fraud, waste, and abuse. PHC's commitment to detecting and preventing fraud, waste, and abuse is further detailed in *Attachment A*, Fraud Prevention Program. ~~These requirements shall be met through the following:~~
   - ~~a. Written policies and procedures that articulate PHC's commitment to comply with all applicable requirements and standards under the contract and all applicable federal and State requirements;~~
   - ~~b. The designation of a Compliance Officer who is responsible for developing and implementing policies, procedures, and practices designed to ensure compliance with the requirements of the contract and who reports directly to the Chief Executive Officer and the Board of Directors;~~
   - ~~c. The establishment of a Regulatory Compliance Committee on the Board of Directors and at the senior management level charged with overseeing PHC's compliance program and its compliance with the requirements under the contract;~~
   - ~~d. A system for training and education for the Compliance Officer, and PHC's workforce members, on the federal and State standards and requirements under the contract;~~
   - ~~e. Effective lines of communication between the Compliance Officer and PHC's workforce members;~~
   - ~~f. Enforcement of standards through well-publicized disciplinary guidelines;~~
   - ~~g. Establishment and implementation of a system with dedicated staff for routine internal monitoring and auditing of compliance risks, promptly responding to compliance issues as they are raised, investigation of potential compliance problems as identified in the course of self-evaluation and audits, correction of such problems promptly and thoroughly, or coordination of suspected criminal acts with law enforcement agencies to reduce the potential for recurrence, and ongoing compliance with the requirements under the contract.~~

B. PHC Workforce Member and Affiliate Responsibilities

1. Every PHC workforce member and affiliate, shall comply with applicable statutes, regulations, rules, and contractual obligations related to the delivery of covered services, which include, but are not limited to, federal and state False Claims Acts, Anti-Kickback statutes, prohibitions on inducements to beneficiaries, Health Insurance Portability and Accountability Act (HIPAA) and other applicable statutes.
2. Every PHC workforce member shall complete regulatory and compliance training at the time of onboarding and annually thereafter and in compliance with PHC policy and procedure CMP-28 Training Program Requirements. This training will include the requirement to report compliance incidents, including potential or actual FWA, to Regulatory Affairs and Compliance (RAC) upon discovery.
3. Every PHC workforce member has the responsibility to understand their job functions and associated processes in order to identify irregularities in the practices of PHC's providers, members or employees,

and to report any potential or actual FWA to RAC. Potential or actual FWA must be reported immediately. PHC workforce members and affiliates shall not defer, delay or not report an incident on the assumption that another individual or department at PHC will make the report.

C. Fraud Detection

1. PHC's approach to identifying and monitoring potential or actual fraud activity is multi-faceted. Each department is responsible for taking proactive steps to monitor for irregularities and detect potential or actual fraud. These department responsibilities are further detailed in the PHC Fraud Prevention Program, which is incorporated into the PHC Compliance Plan. Some of the detection sources include, but are not limited to:

    a. PHC's Compliance Hotline, or other reporting mechanisms;
    b. Claims data history;
    c. Encounter data;
    d. Member and provider complaints, appeals, and grievance reviews;
    e. Medical Records Audits;
    f. Pharmacy data and claims utilization;
    g. Utilization Management reports;
    h. Provider utilization profiles;
    i. Monitoring and auditing activities which may include tracking suspended providers, changes in provider's circumstances that may affect their eligibility to participate in the Medi-Cal program, including terminations of their provider agreement and changes in member eligibility including changes in the member's residence, income and the death of a member;
    j. Monitoring external health care FWA cases and determining if PHC's FWA program can be strengthened with information gleaned from the case activity; and/or
    k. Internal and external survey, review and audits.

B. Procedure

A. Reporting to RAC

1. Upon discovery, PHC Workforce members and affiliates, are required to immediately report all potential or actual incidents of fraud, waste, or abuse to RAC or PHC's Compliance Officer.
2. Potential or actual incidents of FWA shall be reported immediately by:
    a. Internal workforce: Completing the EthicsPoint RAC Intake Form (accessible through PHC's intranet, PHC4Me, or
    b. External parties: Completing a referral using PHC's Incident Reporting form (available on PHC's external website www.partnershiphp.org) and submitting the completed form by email to RAC_Reporting@partnershiphp.org, or
    c. By calling the toll-free Compliance Hotline number at (800) 601-2146, anonymously, or
    d. Contacting any member of PHC management, RAC, or the PHC Compliance Officer.
3. Referrals shall be made immediately upon the initial discovery and must contain all information known to the reporting party including, but limited to, the initial date of discovery by PHC or PHC workforce member(s) or/affiliate(s) and any pertinent details as to the reason the potential fraud, waste or abuse is suspected. Additional information including any, attachments and/ or updates on previously reported referrals may be submitted through any of the previously mentioned reporting mechanisms
4. Any PHC workforce member or affiliate who makes a report in good faith is not subject to retaliation, intimidation, or any other form of reprisal in accordance with PHC policy and procedure CMP-27 Non-intimidation & Non-retaliation.

B. Internal Investigations and Regulatory Reporting Requirements
   1. Upon receiving a report of potential or suspected FWA, RAC will review the referral and conduct a preliminary investigation of the case. During the preliminary investigation, RAC may, when appropriate, refer the case to another PHC unit or department for additional investigation or to determine the validity of the allegation of potential or actual FWA.
   2. PHC's Compliance Officer, or designee, may follow up with the reporting party, as necessary to clarify the initial referral, obtain additional information, or take prompt corrective action to mitigate any risks or damages involved with the actual or potential FWA and to protect the operating environment. Follow up requests may be sent from EthicsPoint directly, or via email
   3. If a case does not relate to PHC programs and/or is inappropriate for PHC investigation, case may be closed without further investigation or referred to DHCS for further investigation.
   4. In accordance with DHCS Contract Exhibit ~~E~~A, Attachment ~~2~~III, ~~Provision 27 (C)(7)~~section 1.3.2(D) PHC shall promptly refer all potential or actual FWA to the DHCS Audits and Investigations Intake Unit..
      a. PHC shall conduct, complete and report to DHCS the results of the preliminary investigation of potential FWA within ten (10) working days from the date RAC, PHC workforce members or affiliates first became aware of, or were in notice of, such activity.
      b. If PHC's preliminary investigation cannot be completed within ten (10) working days, PHC shall report to DHCS with available findings, and provide an updated report with final investigation findings within ten (10) working days once investigation has concluded.
   5. All FWA referrals to DHCS, shall be made on the Medi-Cal Form MC-609: Confidential Report form. The MC-609 form and attachments submitted to DHCS must, at minimum, include:
      a. Number of complaints of fraud and abuse submitted that warranted preliminary investigation
      b. For each compliant which warranted a preliminary investigation, supply:
         i. Name and/or SSN or CIN;
         ii. Source of Compliant;
         iii. Type of Provider (if applicable);
         iv. Nature of compliant;
         v. Approximate dollars involved if known; and
         vi. Legal and administrative disposition of the case
   6. The MC-609 form and all supporting documentation shall be provided to DHCS via secure email to PIUcases@dhcs.ca.gov with a 'cc' to PHC's DHCS Contract Manager.

C. Remediation of founded Fraud, Waste, or Abuse
   1. Overpayments
      a. In accordance with 42 CFR §438.608 and processes established under PHC policy and procedure FIN-~~700~~-405, RAC, with the Finance Cost Avoidance Unit, shall promptly report to DHCS all overpayments identified or recovered due to potential fraud and shall pursue recoveries of any overpayments related to identified FWA activities
   5. Corrective Action
      b. PHC shall promptly communicate, in writing, any identification of founded FWA to the entity in violation describing the violation in detail and the requirements and timeframe for the implementation of corrective action that may include the imposition of administrative or financial sanctions.
   6. Imposition of Sanctions
      c. PHC may, in addition to any recoupment of overpayment, applicable civil penalties accessed by regulatory agencies, or the implementation of corrective action, may impose administrative or financial sanctions against the entity in violation and in accordance with PHC policy and procedure ADM-47 Administrative and Financial Sanctions.

B. Confidentiality and Records Retention
   1. All referrals and subsequent investigation of FWA are conducted in a manner which protects the reporting party's confidentiality to the extent reasonable for the purposes of the investigation and in accordance with PHC policy and procedure CMP-10 Confidentiality.
   2. All data, information, and documentation related to FWA referrals and investigations are retained in accordance with PHC policy CMP-30 Records Retention and Access Requirements.

II. REFERENCES:

A. Compliance Plan
B. DHCS Contract ~~08-85215~~23-30236, Exhibit ~~E~~A, Attachment ~~2~~III, ~~Provision 27(B)(C)~~Section 1.3
C. Title 42 CFR 455.2, 438.608 and 438.610
D. Welfare and Institutions Code 14043.1

III. DISTRIBUTION:

A. PowerDMS

IV. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE:

Compliance Officer

V. REVISION DATES:

Medi-Cal
12/06/11, 12/04/12, 03/26/13, 09/01/15, 09/07/16, 05/17/17, 05/24/2018, 05/16/2019, 02/20/2020, 02/18/2021, 02/17/2022, 02/16/2023, 02/15/2024

PREVIOUSLY APPLIED TO:

PartnershipAdvantage:
CMP-09 – 03/02/2010 to 01/01/2015
Healthy Families:
CMP-09 – 10/01/2010 to 03/01/2013
Healthy Kids
CMP-09 – 12/06/2011 to 12/31/2016

Policy/Procedure Number: CMP-20 (Formerly ADM-22)				**Lead Department: Administration**	
Policy/Procedure Title: Brown Act Compliance				☐ **External Policy** ☒ **Internal Policy**	
Original Date: 09/01/2009			**Next Review Date:** ~~**12/02/2022**~~ **Last Review Date:** ~~**12/02/2021**~~		
Applies to:	☒ **Medi-Cal**		☐ **Healthy Kids**	☐ **Employees**	
Reviewing Entities:	☐ **IQI**		☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**		☐ **EXECUTIVE**	☐ **COMPLIANCE**	☐ **DEPARTMENT**
Approving Entities:	☒ **BOARD**		☒ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO**	☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: ~~*Elizabeth Gibboney*~~*Sonja Bjork*				**Approval Date: 12/02/2021**	

I. RELATED POLICIES:

N/A

II. IMPACTED DEPTS.:

All

III. DEFINITIONS:

A. Posted: Notices of meetings, including agendas, must be posted 72 hours prior to the meeting in a location that is accessible 24 hours a day for the 72 hours prior to the meeting.

B. Teleconference meeting: A teleconference meeting is a meeting in which one or more members of the Board attend the meeting from a remote location via electronic means, transmitting audio or audio/video.

IV. ATTACHMENTS:

A. PHC Regularly Scheduled Meetings

V. PURPOSE:

To ensure compliance with the Ralph M. Brown Act.

VI. POLICY / PROCEDURE:

A. Policy.

1. As defined in California Government Code section 54952(b), governing subsidiary bodies of the Board may be subject to the Ralph M. Brown Act. In accordance with this Act, the meetings listed in Attachment A are designated as either closed or open to the public.
2. Interested members of the public, including, but not limited to the media, members of Partnership HealthPlan of California and other concerned individuals may attend meetings listed as open to the public. Portions of meetings may be closed to the public pursuant to closed sessions criteria set forth in Government Code section 54950, et seq.
3. Regularly scheduled meeting are subject to notice and agenda requirements pursuant to California Government Code section 54954.2.
4. Pursuant to California Government Code section 54953(b)(1) (AB 2449?) and through January 1, 20~~2~~26~~24~~, ~~all~~ there are limited circumstances allowing meetings ~~may~~ to be held via teleconferencing, outside of the general (pre-pandemic) Ralph M. Brown Act teleconferencing requirements. ~~as long as they comply with the other requirements of the Ralph M. Brown Act~~

B. Procedure.

1. Agendas for regularly scheduled meetings shall be posted at least 72 hours prior to the meeting on the PHC website and publically at the PHC's meeting locations, including all teleconference call locations.
2. 24hour notice will be provided in the case of special meetings. One hour notice may be provided in the case of an emergency meeting, unless that meeting is held due to a dire emergency. If requested, the agenda shall be made available in appropriate alternative formats to persons with a disability, as required by Section 202 of the Americans with Disabilities Act of 1990 (42 U.S.C. Sec. 12132), and the federal rules and regulations adopted in implementation thereof.
3. The agenda shall include information regarding how, to whom, and when a request for disability-related modification or accommodation, including auxiliary aids or services, may be made by a person with a disability who requires a modification or accommodation in order to participate in the public meeting.
4. All other meetings are closed to the public as specified. Requirements for agenda for closed meetings are listed under Attachment A.
5. If Board or committee members participate in meetings via a teleconference location, each teleconference location must be fully accessible to members of the public and the procedure for posting the agenda, listed in section (1) above, must be followed.

VII. REFERENCES:

California Government Code Section 54950 et. seq., (also known as the Ralph M. Brown Act.)

VIII. DISTRIBUTION:

A. ~~SharePoint~~PowerDMS
B. Directors

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE:

A. Department contacts are responsible for ensuring department compliance with Brown Act.
B. Compliance Department is responsible for auditing compliance with Brown Act.

X. REVISION DATES / APPROVED BY BOARD:

Medi-Cal

A. 06/18/10, 12/06/11, 12/04/12, 03/26/13, 8/26/15, 09/07/16, 05/17/2017, 08/23/2018, 12/04/2019, 11/19/2020, 12/02/2021
B. Board Resolution 3.6 on 6/28/17
C. Board Resolution 3.6 on 12/04/2019

PREVIOUSLY APPLIED TO:

PartnershipAdvantage:
CMP-20 – 09/01/2009 to 01/01/2015
Healthy Families:
CMP-20 – 10/01/2010 to 03/01/2013
Healthy Kids:
CMP-20 – 06/18/2010 to 12/31/2016

Policy/Procedure Number: CMP-20 (Formerly ADM-22)			**Lead Department: Administration**
Policy/Procedure Title: Brown Act Compliance			☐ **External Policy** ☒ **Internal Policy**
Original Date: 09/01/2009		**Next Review Date: 12/02/2022** **Last Review Date: 12/02/2021**	
Applies to:	☒ **Medi-Cal**	☐ **Healthy Kids**	☐ **Employees**

ATTACHMENT A

REGULARLY SCHEDULED ~~PHC~~ PUBLIC PARTNERSHIP MEETINGS

Revised ~~5/12/2017~~02/07/2024

MEETING	Open or Closed?	Agenda Publicly Posted?
External/Commission		
~~340B Advisory Committee~~	~~Open~~[1]	~~Yes~~
Commission (Board)	Open[1]	Yes
Compliance / Governance Committee	Open[1]	Yes
CEO Evaluation Committee	Closed[4]	No
Consumer Advisory Committee (CAC)	Open[1]	Yes
Credentialing	Closed[3]	No
Family Advisory Committee	Closed	No
Finance Committee	Open[1]	Yes
Peer Review (sub-committee of Q/UAC)	Closed[3]	No
Physicians Advisory Committee	Open[1]	Yes
Provider ~~Advisory~~ Engagement Group (PEAG)	~~Open~~[1]Closed	~~Yes~~No
Quality Improvement and Health Equity Committee	Closed	No
Quality/Utilization Advisory Committee (Q/UAC)	Open[2]	Yes
Strategic Planning Committee	Open[2]	Yes
Personnel, Policies and Benefits Committee	Open[2]	Yes

[1] This meeting is open if the Committee was created by the Commission (charter, ordinance, resolution, formal action or Bylaws) and/or Commissioners have an official seat.

[2]This meeting is open because it is a standing committee which has jurisdiction over a particular subject area.

[3]This meeting is closed under CA Evidence Code §1157.

[4]This meeting is closed under CA Government Code §54957.

Note: Meetings can also be considered closed if it is a meeting of a committee that is non-standing, advisory and is comprised only of less than a quorum of members of the Commission.

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

Policy/Procedure Number: CMP-39				**Lead Department: Compliance**	
Policy/Procedure Title: Regulatory Change Management				☐ **External Policy** ☒ **Internal Policy**	
Original Date: 08/15/2019			**Next Review Date:** ~~02/16/2024~~02/15/2025 **Last Review Date:** ~~02/16/2023~~02/15/2024		
Applies to:	☒ **Medi-Cal**		☐ **Healthy Kids**	☒ **Employees**	
Reviewing Entities:	☐ **IQI**		☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**		☐ **EXECUTIVE**	☒ **COMPLIANCE**	☐ **DEPARTMENT**
Approving Entities:	☐ **BOARD**		☒ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO**	☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: ~~*Elizabeth Gibboney*~~*Sonja Bjork*				**Approval Date:** ~~02/16/2023~~02/15/2024	

I. RELATED POLICIES:

A. CMP-03 Compliance Approval Process

B. CMP-30 Records Retention and Access Requirements

~~B.~~C. CMP36 Delegation Oversight and Monitoring

II. IMPACTED DEPTS:

A. All

III. DEFINITIONS:

A. Change Management: Process for assessing ~~impact~~ and responding to ~~of~~ regulatory guidance informing ~~to~~ PHC operations, services, payment structure, and/or contractual relationships, including those with Subcontractors and Delegates and supports change with minimal disruption.

B. Delegate: An external entity that PHC has given the authority to perform an activity/activities that PHC would otherwise perform as defined by the National Committee for Quality Assurance (NCQA) standards. By virtue of performing delegated activities, a delegate is always a subcontractor.

C. Subcontractor: A person or entity who enters into a subcontract with PHC. Assessing whether an entity is a Subcontractor depends on the relationship between the entities and the services being performed, not on the type of persons or companies involved. A person or entity is deemed a subcontractor if: 1) they are either a provider of health care services that agreed to furnish Covered Services to PHC Members, or 2) has agreed to perform any administrative function or service for PHC specifically related to fulfilling PHC's obligations to DHCS under the terms of the DHCS/Medi-Cal contract.

IV. ATTACHMENTS:

A. Regulatory Guidance Index

B. Regulatory Implementation Checklist

C. Regulatory Change Management RACI

V. PURPOSE:

To establish guidelines for Partnership HealthPlan of California's (PHC) implementation of regulatory guidance and/or nationally recognized accreditation standards, as applicable. This policy supports PHC's timely and comprehensive compliance with federal and state statutes, regulations, contractual obligations, and rules by defining a consistent approach to managing regulatory change. Benchmarks and processes described under this policy should serve as recommendations unless otherwise specified where regulatory authority is provided.

Policy/Procedure Number: CMP-39		Lead Department: Compliance	
Policy/Procedure Title: Regulatory Change Management		☐ External Policy ☒ Internal Policy	
Original Date: 08/15/2019		Next Review Date: 02/16/202402/15/2025 Last Review Date: 02/16/202302/15/2024	
Applies to:	☒ Medi-Cal	☐ Healthy Kids	☒ Employees

VI. POLICY / PROCEDURE:

A. Policy

1. Governance of Regulatory Change Management:
   a. PHC, a managed care health plan (MCP), contracted with the Department of Health Care Services (DHCS), is governed by DHCS contractual obligations, written guidance, laws, and regulations applicable to the State of California's Medi-Cal program which includes, but is not limited to:
      1) DHCS contract and subsequent amendments
      2) DHCS All Plan Letters (APL)
      3) DHCS California Children's Services (CCS) Numbered Letters (N.L), as applicable under APL 18-023
      4) DHCS Behavioral Health Instructional Notices (BH IN) as applicable to the Drug-Medi-Cal Organized Delivery System (DMC-ODS);
      5) DHCS Fee-for-Service (FFS) provider manual, as applicable
      6) California Code of Regulations, Title 22
      7) Code of Federal Regulations, Title 42, Chapter IV
      8) California Code of Regulations, Title 28, as applicable and directed by contract with DHCS
   b. *Attachment A Regulatory Guidance Index* provides reference to common issuing agencies, methods of issuance, and PHC's obligation to comply with guidance.

2. Responsibility for Implementation of Regulatory Change: the following is a detailed description of key roles and responsibilities of regulatory change management participants. *Attachment C* to this policy provides a RACI as an overview/visual reference of roles/responsibilities.

   a. **Regulatory Affairs and Compliance (RAC):** RAC is responsible for receiving and maintaining record of regulatory guidance provided directly from DHCS including, but not limited to, DHCS contract amendments, APLs, BH Ins, NLs, and other written guidance. RAC will perform an initial impact assessment to determine which PHC departments are impacted and route accordingly. RAC will work with key departments to determine applicability to PHC subcontractors and/or delegates and communicate externally as appropriate. RAC will ensure guidance materials are made available upon release by DHCS.
   b. **Department Director**: Each PHC department director is responsible for ensuring that their department implements regulatory guidance in a manner and timeframe consistent with the regulatory guidance and where possible, in alignment with processes described under this policy and procedure. Department directors are responsible for designating a business owner and one back-up to support regulatory implementation activities. Department directors should notify RAC within fourteen (14) business days when there is a change in designation.
   c. **Business Owner**: Each PHC department shall designate a business owner to support implementation and cross-departmental/regional collaboration. Business owners should be familiar with department operations and have contextual understanding of subject matter and applicability of regulatory guidance. This person is responsible for~~designated to receive~~ receiving guidance from RAC, assessing impact, and supporting/facilitating~~e~~ department implementation and validation activities. This person promotes~~,~~ adherence with~~to~~ requirements of regulatory guidance and established PHCs processes like those described under this policy

and procedure, benefit implementation, and applicable department desktop policies and procedures. Business owners are responsible for participating in regulatory change management meetings, engaging in discussion, providing updates on department implementation activities and collaborating with other departments as necessary.

3. Timeliness of Regulatory Implementation:
   a. When applicable, impacted PHC departments shall make necessary programmatic and/or operational changes in a manner and timeframe consistent with that required by regulatory~~the~~ guidance and/or PHC leadership. This may include completion and submission of deliverables to regulatory agencies. When an implementation date is not specified by regulatory guidance, the recommended period for timely completion is based on the release date of regulatory guidance and/or the effective date of such guidance.
      1) ~~Pursuant to DHCS contract 08-85215, Exhibit A, Attachment 18,~~ PHC shall make updates to materials, guides, and/or deliverables and submit to DHCS for review and approval within timeframes specified by finalized DHCS guidance or ~~thirty (30) days of the release of final contractual amendments or a~~s otherwise specified by regulatory and/or statutory rules.
      2) Where timeliness of implementation are ~~is~~ not indicated by regulatory guidance, PHC departments shall make ~~their~~ best efforts to apply change within a reasonable amount of time. What is reasonable may depend on what changes ~~must be made to be in~~are necessitated for compliance. Reasonable timeframes for completion of updates (from the date of release of final guidance):
         a. Updates to member materials – reasonable to update within thirty (30) calendar days (this suggested timeframe does not include review by committee or submission to DHCS, as applicable)
         b. System configuration – reasonable to submit an IT support request and have system changes, as applicable scheduled within sixty (60) calendar days
         c. Amendments to subcontractor/delegate agreements – reasonable to issue a memo describing the regulatory changes sixty (60) days prior to the effective date of the change or within one (1) week of receipt of guidance when early notification is not feasible
         d. Updates to policies and procedures/desktops – reasonable to update within sixty (60) calendar days
      3) In the instance that any PHC department foresees a challenge with implementing regulatory guidance within the specified timeframe, including instances where deliverables cannot be timely submitted to DHCS, the responsible department must make a written report to RAC. To submit a written report:
         a. Submit via email to RegulatoryGuidance@partnershiphp.org and include:
            i. Name of related guidance;
            ii. Name of delayed material or implementation activity;
            iii. Department(s) not able to meet the specified timeframe;
            iv. Detailed description of the reason for delay;
            v. If requesting an extension – specify proposed due date;
            vi. Detailed description of support or clarification needed; and
            ~~i.~~vii. Include department director as proof of leadership endorsement for delayed implementation.

4. Regulatory Implementation Internal Controls:
   a. PHC departments are to maintain desktop policies and procedures that describe the process to evaluate and respond to finalized regulatory guidance, including which positions within the department are responsible for the implementation process.
   b. To support collaboration and comprehensive understanding of requirements, a standing regulatory change management meeting convenes as frequently as once monthly or as necessitated by the cadence with~~frequency in~~ which guidance is released. This meeting is hosted by Regulatory Affairs and Compliance (RAC) and includes each department business owner.
      1) This meeting serves as a venue for regulatory guidance discussions; including making progress reports, issue spotting, and needs for support in implementation. The workgroup does not serve as a working meeting to manage the implementation of regulatory guidance. Departments are expected to ~~s and does not preclude departments from engaging in~~engage in implementation activities in a timely manner and outside of the monthly meeting. ~~Departments should use the regulatory change management meeting to provide status updates, challenges, and needs for their implementation of guidance.~~
      2) RAC may participate in or facilitate ad hoc/focused meetings outside of the standing workgroup~~workgroups~~ as necessary.
   c. To guide implementation activities, when appropriate, regulatory guidance shall be categorized into one and/or many of the following implementation types:
      1) **Benefit Implementation** – Mandates the provision of a new Medi-Cal benefit
      2) **Administrative** – Requires changes to PHC operational and/or administrative activities such as payment structures, policies and procedures, or management information systems
      3) **Scope of Services** – Makes changes to the delivery or coverage of current Medi-Cal services but does not mandate a new benefit
      4) **Subcontractor/Delegate Oversight** – Directly mandates oversight obligations specific to subcontracted or delegated functions or adds or changes the scope of services, benefits, or administrative responsibilities of subcontractors/delegates for which PHC will be responsible for overseeing

B. Procedure
1. Circulation of Regulatory Guidance:
   a. Within four (4) business days from receipt of regulatory guidance, RAC shall perform an initial impact assessment, including recommended implementation type, and route to applicable department business owners and/or, department directors.
      1) This circulation will include the final guidance and an implementation checklist that specifies impacted departments and regulatory guidance implementation type for department use.
      2) RAC will distribute and maintain record of guidance summaries and DHCS review tools/resources as available.
      3) RAC will communicate regulatory guidance to subcontractors/delegates.

2. Department Implementation:
   a. Upon receipt of guidance, business owners are responsible for internal department dissemination and assessment.
      1) Departments are expected to review, identify necessary changes, and assign responsibility as appropriate. Such assessment should be guided by *Attachment B, Regulatory Implementation Checklist*.

2) Departments are responsible for maintaining record of updated materials as necessitated by final guidance.

b. Departments are required to make regular reports of implementation updates to the regulatory change management workgroup. Updates should include but not be limited to:
   1) Updating written materials;
   2) Education to providers, subcontractors, and staff;
   3) Reporting to DHCS; new and amended;
   4) System impacts; updates made and planned; and
   5) Cross-departmental collaboration.

~~b.~~c. Departments are responsible for engaging implementation partners as necessary, including, but not limited to:
   1) RAC as needed for guidance, clarification, and/or regulatory implementation activities such as workgroups, except where otherwise indicated by RAC. RAC will assume an active role in implementation activities without department request when such guidance has a global impact (i.e. restatement of DHCS contract);
   2) Project Management Office (PMO) when implementation activities require support from a project manager or review by the Project Review Board (PRB);
   3) Claims and/or configuration where changes to the claims system are necessary;
   4) Communications and Health Education where amendments to current or development of new member materials are required;
   5) IT where system changes or expansions are required;
   6) Contract Administration/Provider Relations where creation of a new or amendment to an existing subcontractor/delegate or network provider agreement is required; and
   7) Finance where changes to an entities responsibilities (typically through contract amendment) will result in a change the entities financial reimbursement

~~c.~~d. Departments are responsible for developing and/or, amending, materials ~~when a deliverable is required by~~as necessitated by final regulatory guidance. Mandatory d~~D~~eliverables shall be developed and submitted in compliance with PHC Policy and Procedure CMP-03 Compliance Approval Process, including, but not limited to, department's responsibility to:
   1) Submit required deliverables to RegulatoryGuidance@partnershiphp.org on or before the specified internal due date;
      a) If the deliverable submitted is an amended document, changes must be reflected in track changes (this is not applicable to newly developed materials).
      ~~a)~~b) If the deliverable submitted was previously approved by DHCS, department must clearly indicate what has changed from prior submission.
   2) Completing and submitting DHCS review criteria work sheet, as available;
   ~~2)~~3) Maintaining record of updated materials, submission to RAC for review and approval by DHCS, and outcome of DHCS review; and
   ~~3)~~4) Respond to RAC and/or DHCS additional information requests (AIR) related to a deliverable in the manner and timeframe specified within the AIR. Requests for an extension shall be communicated by the department and facilitated by RAC.

3. Validation of Implementation
   a. In demonstration of satisfactory implementation and compliance with regulatory guidance, PHC departments will provide written acknowledgement of implementation once activities are complete. This acknowledgement will be completed through department director and business owner written acknowledgement via email ~~and/or sign off of~~ submission of the completed

implementation checklist.

1) If a deliverable to a regulatory agency is required under implementation, said deliverable must be submitted to RegulatoryGuidance@partnershiphp.org on or before the specified internal due date with a completed implementation checklist.
2) If no deliverable is required, the completed implementation checklist shall be provided to RAC via email within five (5) business days of completed implementation. Departments may consult with RAC regarding regulatory activities during the course of implementation as needed.
3) Departments are expected to retain record of implementation validation

b. Validation of satisfactory implementation may be conducted through any of the following mechanisms including, but not limited to, regular internal oversight and monitoring, DHCS approval of required deliverables, and/or auditing.

4. Record Retention:
   a. Data, documentation, and information related to the processes described under this policy shall be maintained in compliance with PHC policy and procedure CMP-30 Records Retention and Access Requirements.

VII. REFERENCES:

~~DHCS contract 08-85215~~

VIII. DISTRIBUTION:

1. PowerDMS

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE:

A. Department Directors
B. Regulatory Affairs and Compliance

X. REVISION DATES:

11/19/2020, 12/02/2021, 02/16/2023, 02/15/2024

PREVIOUSLY APPLIED TO:

N/A

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY / PROCEDURE

<table>
<tr><td colspan="3">Policy/Procedure Number: CMP-03</td><td colspan="3">Lead Department: Regulatory Affairs and Compliance</td></tr>
<tr><td colspan="3">Policy/Procedure Title: Compliance Approval Process</td><td colspan="3">☐ External Policy
☒ Internal Policy</td></tr>
<tr><td colspan="2">Original Date: 06/05/2007</td><td colspan="4">Next Review Date: ~~02/17/2023~~02/15/2025
Last Review Date: ~~02/17/2022~~02/15/2024</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: ~~Elizabeth Gibboney~~Sonja Bjork, CEO</td><td colspan="3">Approval Date: ~~02/17/2022~~02/15/2024</td></tr>
</table>

I. RELATED POLICIES:

A. COM-03 Communications Standards
B. MPHP Health Education Program
C. CMP39 Regulatory Change Management

II. IMPACTED DEPTS.:

All.

III. DEFINITIONS:

A. Health education materials: informing documents designed to assist members modify personal health behaviors, achieve and maintain healthy lifestyles, and promote positive health outcomes by including information on health conditions, management of health conditions, and self-care.
B. Member informing materials: vital documents that provide PHC members with essential information about access to and usage of PHC services. Member information shall include the Member Services Guide (EOC), provider directory, significant member mailings and notices, and any notices related to the grievances, actions, and appeals.
C. File and Use: a submission to DHCS that does not need review and approval prior to use or implementation, but which DHCS can require edits as deemed necessary.

IV. ATTACHMENTS:

Attachment A. DHCS File and Use Attestation

V. PURPOSE:

To establish a process for the review, submission, approval, and processing of member informing materials, and health education materials, as well as other items that may be submitted to DHCS and/or other State and Federal regulatory agencies by the Regulatory Affairs & Compliance (RAC) for PHC's lines of business.

VI. POLICY / PROCEDURE:

A. Policy.
1. As required by DHCS contract ~~08-8521~~23-30236, Exhibit A, Attachment III~~13~~, ~~Provision 4,~~Section 5.1.3 (Member Information) and All Plan Letter (APL) 18-016, PHC shall ensure that all member informing materials are provided to members at a sixth grade reading level or as determined appropriate through PHC's group needs assessment (GNA) and approved by DHCS. As specified by contractual obligations and/or regulatory guidance, some materials may be deemed appropriate for annual file and use submission and do not require DHCS review and approval prior to implementation. Member

information requiring DHCS review and approval shall include, but is not limited to;

a. Member handbook (EOC)
b. Provider directory
c. Significant member mailings and notices including provider termination notices and change in coverage of services
d. Member newsletters
e. Welcome packets
f. Any notices related to grievances, actions, and appeals

2. Materials requiring DHCS review/approval

A. As required by DHCS contract 23-3023608-85215, Exhibit A, Attachment III, Section 1.1.10~~-18~~, PHC shall make updates to materials, guides, and/or deliverables and submit to DHCS for review and approval ~~within 30 days of the release of contractual amendments or as otherwise~~consistent with timeframes specified by regulatory and/or statutory rules and/or guidance. Materials may include, but are not limited to:

i. Newly developed or substantially revised policies and procedures to meet regulatory requirements and/or contractual obligations
ii. Training materials/schedules
~~i.~~iii. Member notices
~~ii.~~iv. Cultural and Linguistics Plan
~~iii.~~v. Population Needs Assessments
~~iv.~~vi. Other documents as specified by the applicable regulatory agency

B. Pursuant to DHCS contract 23-30236, Exhibit A, Attachment III, Section 1.1.10, DHCS reserves the right to review and approve PHC policies and procedures and as such, may require amendments to comply with contractual or regulatory obligations.

i. Materials developed or amended as a result of regulatory guidance or contractual amendment must be submitted consistent with PHC policy CMP39 Regulatory Change Management.

~~2.~~3. File and use materials: Informing materials that are not deemed vital member information are considered health education materials and do not require DHCS review and approval prior to use and are not subject to DHCS file and use requirements. These materials should be reviewed by PHC's qualified health educator as required by DHCS All Plan Letter (APL) 18-016. Health education materials may include but are not limited to:

a. Brochures on health topics or programs
b. Pamphlets informing members of specific health conditions
c. Packets of self-care instructions
d. Guidance for preparing for a procedure
e. Newsletters that focus on health education messages, such as promoting healthy lifestyles and behaviors

4. PHC shall develop member informing materials, health education materials, policies and procedures, and other materials as specified by State or Federal program requirements and in compliance with PHC policy and procedure COM-03 Communications Standards.

~~3.~~5. As allowable by DHCS and for those materials that do not require DHCS review and approval before use, PHC may submit materials to DHCS as file and use. Submission as file and use does not preclude DHCS from requiring the plan make edits to or terminate use of materials. Materials that may be considered for file and use include and are consistent with Attachment A. DHCS File and Use Attestation, this includes but is not limited to:

~~A. Policies and procedures not specified by DHCS as contractual requirement or an APL deliverables;~~

~~B. Minor updates to policies and procedures required by DHCS (updates must be made in track changes (redline))~~

i. ~~Minor edits mean those that do not impact PHC's compliance with legal and contractual requirements, DHCS policy, and DHCS guidance~~

~~C.~~B. Minor edits to deliverables/submissions that were already reviewed and approved by DHCS within the last six months

i. These edits must be made and submitted with track changes (redline) and prior DHCS approval attached

ii. Minor edits mean those that do not impact PHC's compliance with legal and contractual requirements, DHCS policy, and DHCS guidance; or

~~D.~~C. Consent forms such as authorized representative forms and minor consent forms

~~4.~~6. The department responsible for the development, maintenance, and submission (to RAC) of materials, is responsible for declaring if the material is member informing or health education and whether they believe the submission meets file and use criteria.

A. If file and use criteria is met, Attachment A. DHCS File and Use Attestation, must be completed and included with RAC's submission to DHCS

~~5.~~7. RAC shall review all member informing materials, developed with regard to benefits, intended to be distributed to PHC members prior to submission to DHCS and/or other regulatory agency.

~~6.~~8. RAC shall submit all PHC-approved materials to DHCS and/or other regulatory agency for review and approval or file and use as appropriate.

~~7.~~9. RAC shall maintain a regulatory submission log of member informing materials and PHC materials and/or guides to track and distribute DHCS and/or other regulatory agency review decision to the respective PHC department(s) and/or the Compliance Committee.

~~8.~~10. While developing and/or amending any of the above mentioned member informing materials, health education materials, and/or PHC materials and/or guides, PHC departments may, as they deem necessary, request RAC or DHCS and/or other regulatory agency interpretation and clarification of regulatory requirements. This process is separate from the compliance approval process noted below. The return of any documents with clarification should not be misconstrued as an approval for submission to the reviewing regulatory agency. Documents must be finalized as detailed in the compliance approval process before submission to regulatory review agency.

B. Procedure

1. The PHC department submitting materials for RAC and/or DHCS review shall provide, in final form, the material requiring submission to DHCS, in either MSWord (.doc) or Adobe Acrobat (.pdf) format via e-mail to RAC_Inbox@partnershiphp.org.
    a. The submitting department should indicate if the material is member informing or health education and whether they believe the submission meets file and use criteria
2. If the material to be reviewed is intended to be used as a template, it must include the required placeholder(s) to be populated by specific text. For example: <Name>; <Date>; etc.
3. Upon receipt, RAC shall:
    a. As applicable, review materials for adherence to regulations, proper proposed use, and completeness;
        1) Review the material to determine if it is considered health education material or meets file and use criteria.
        2) If the material is considered health education, it shall be returned to the submitting

department, with reminder of the requirements outlined in section A(3) of this policy.

3) If the material meets file and use criteria, RAC shall complete Attachment A. DHCS File and Use Attestation, acquiring necessary signatures and ensuring the completed form is included with the DHCS submission;

b. Assign a submission specific reference number and log the material by file name and originating department, and indicate if the material is file and use or standard review on the DHCS Submission Tracker. The tracker is accessible on the Regulatory Affairs SharePoint page;

c. Submit material to DHCS and/or any other regulatory agency as applicable, for review and approval or as file and use;

d. Email PHC originating department with the assigned reference number and confirmation of regulatory submission; and

e. Maintain copies of the original materials as submitted to RAC and subsequent submission to the reviewing regulatory agency.

4. Once approved by DHCS and/or other regulatory agency, an email confirmation of approval will be forwarded to the originating PHC department.
5. Upon initial review, if the material is not approved by DHCS and/or other regulatory agency, it will be returned to the originating PHC department with comments for correction and/or a request for additional information (AIR).
6. Per DHCS contract -23-30236, Exhibit A, Attachment III, Section 1.1.10~~08-85215, Exhibit E, Attachment 3, Provision 5,~~ DHCS shall make all reasonable efforts to review materials submitted by PHC within 60 days of receipt. If DHCS does not complete its review of submitted material within 60 calendar days of receipt, PHC may elect to implement or use the material understanding the material is subject to possible subsequent correction and/or disapproval by DHCS.
7. DHCS rejection or requested amendment of materials.
    a. Materials submitted to the RAC incomplete, incorrect, or missing information will be returned to the originating department and may not be implemented or distributed until final approval by RAC and/or DHCS is received.
    b. Materials returned from DHCS, notated non-approved, shall be reviewed by RAC for comments and returned by email to the originating department for correction. This includes materials submitted as file and use.
    c. Response from originating department is due back to RAC on or before the designated due date set forth by DHCS on the denial and/or AIR.
    d. If changes or a response cannot be made by the designated due date on the DHCS AIR, originating department must notify RAC to request an extension.
    e. Extension request should include the reason for the request as well as the proposed extended due date being requested. Extensions are subject to DHCS or regulatory agencies approval.

VII. REFERENCES:

A. Title 22

B. DHCS contract 23-3023608-85215:

~~1. Exhibit A, Attachment 13~~

~~2. Exhibit A, Attachment 18~~

~~3. Exhibit E, Attachment 3~~

C. DHCS All Plan Letter (APL) 18-016

VIII. DISTRIBUTION:

A. SharePoint

B. Directors

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE:
Compliance Officer

X. REVISION DATES:
Medi-Cal
03/02/2010, 09/06/2011, 12/01/2015, 12/06/2016, 02/22/2018, 03/07/2019, 02/20/2020, 02/18/2021, 02/17/2023, 02/15/2024

PREVIOUSLY APPLIED TO:
PartnershipAdvantage:
CMP-3 – 06/05/2007 to 01/01/2015
Healthy Families:
CMP-3 – 10/01/2010 to 03/01/2013
Healthy Kids
CMP-3 – 06/05/2007 to 12/01/2016

State of California—Health and Human Services Agency
Department of Health Care Services

WILL LIGHTBOURNE
DIRECTOR

GAVIN NEWSOM
GOVERNOR

Medi-Cal Managed Care Plan
File and Use Attestation Form

This File and Use Attestation Form (Attestation Form) is required to be completed when _____(Contractor) intends to use or implement any Contractor materials prior to DHCS review and approval (File and Use).

This Attestation Form must be completed by the Chief Executive Officer, Chief Operating Officer, or Compliance Officer. Contractor must submit this Attestation Form whenever Contractor submits a Contractor material for File and Use, and Contractor must attach the Contractor material to this Attestation Form. The following types of Contractor materials may be submitted for File and Use:

- Member preventative care materials, such as flu campaigns and diabetes control
- Outreach materials related to plan proprietary systems, such as member portals and mobile applications
- General modality of outreach proposal, i.e., text, e-mail, Facebook or other social media posts, mobile app notification) with a previously DHCS-approved vendor and DHCS-approved campaign proposal policy and procedure
- Updated policies and procedures with redline edits.

By signing this Attestation Form, Contractor represents, warrants, and attests that the attached Contractor materials labelled as Exhibit(s) _____comply with all federal and state laws, regulations, guidance, and contractual requirements as set forth in the Medi-Cal Managed Care Contract (Contract) between the Department of Health Care Services (DHCS) and Contractor. Contractor certifies that the attached Contractor materials are complete and accurate.

Contractor retains full legal responsibility for the use of the attached Contractor materials and agrees to indemnify and hold DHCS harmless for any damages or injuries resulting from the use of the attached Contractor materials.

Contractor acknowledges DHCS retains all of its rights under the Contract, including but not limited to, its right to review, modify, stop, approve, or deny the Contractor's right to use the attached Contractor materials. Alternatively, Contractor acknowledges DHCS' right to require Contractor to edit the Contractor materials at any time.

Attestation

I hereby attest on behalf of _____(Contractor) that is has complied with and will continue to comply with all requirements set forth above.

Signature _____Date _____

_____
(Name of CEO, COO, or Compliance Officer)

_____
(Printed Name of Contractor)

_____
(City, State)

The following shall have the same legal force and effect as an original of the signed Attestation Form: a facsimile, photocopy, imaged or other electronic version.

When completed, please send the signed Attestation Form to your assigned DHCS Contract Manager.

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY / PROCEDURE

<table>
<tr><td colspan="4">Policy/Procedure Number: CMP-21 (Formerly ADM-23)</td><td colspan="3">Lead Department: Administration</td></tr>
<tr><td colspan="4">Policy/Procedure Title: Conflict of Interest Code</td><td colspan="3">☒ External Policy
☒ Internal Policy</td></tr>
<tr><td colspan="3">Original Date: 03/12/2010</td><td colspan="4">Next Review Date: ~~02/16/2024~~02/15/2025
Last Review Date: ~~02/16/2023~~02/15/2024</td></tr>
<tr><td>Applies to:</td><td colspan="2">☐ Medi-Cal</td><td>☐ Healthy Kids</td><td colspan="3">☒ Employees</td></tr>
<tr><td rowspan="2">Reviewing Entities:</td><td colspan="2">☐ IQI</td><td>☐ P & T</td><td colspan="3">☐ QUAC</td></tr>
<tr><td colspan="2">☐ OPERATIONS</td><td>☐ EXECUTIVE</td><td>☐ COMPLIANCE</td><td>☐ DEPARTMENT</td></tr>
<tr><td rowspan="2">Approving Entities:</td><td colspan="2">☐ BOARD</td><td>☒ COMPLIANCE</td><td>☐ FINANCE</td><td>☐ PAC</td></tr>
<tr><td>☐ CEO</td><td>☐ COO</td><td>☐ CREDENTIALING</td><td colspan="3">☐ DEPT. DIRECTOR/OFFICER</td></tr>
<tr><td colspan="4">Approval Signature: ~~Liz Gibboney, CEO~~Sonja Bjork, CEO</td><td colspan="3">Approval Date: ~~02/16/2023~~02/15/2024</td></tr>
</table>

I. RELATED POLICIES:

A. HR102 Conflict of Interest

~~B. CMP-17 Glossary of Terms~~

II. IMPACTED DEPTS:

All

III. DEFINITIONS:

N/A

IV. ATTACHMENTS:

A. Exhibit A - Statement of Economic Interest References and Disclosure Categories

B. Exhibit B – Designated Positions

V. PURPOSE:

To reiterate the Conflict of Interest Code that Partnership HealthPlan of California (PHC) adopted on August 24, 2005 as a policy. PHC hereby adopts a Conflict of Interest Code, which incorporates the Model Code by reference, together with Exhibits "A" and "B", for purposes of submission for approval by the Fair Political Practices Commission (FPPC). This shall constitute PHC's Conflict of Interest Code upon obtaining FPPC approval.

Incorporation by Reference of Fair Political Practices Commission ("FPPC") Regulation §18730 (2 California Code of Regulations §18730).

The Political Reform Act (Government Code §81000 et. seq.), requires state and local government agencies to promulgate and adopt conflict of interest codes. The FPPC has adopted a regulation (2 California Code of Regulations §18730) that contains the terms of a standard conflict of interest code, which can be incorporated by reference in an agency's Code. After public notice and hearing, the standard Code may be amended by the FPPC to conform to amendments in the Political Reform Act. Therefore, the terms of 2 California Code of Regulations §18730 and any amendments to it duly adopted by the FPPC are hereby incorporated by reference. This regulation and the attached Appendices, designating positions and establishing disclosure categories, shall constitute the Conflict of Interest Code of Partnership HealthPlan of California.

Policy/Procedure Number: CMP-21 (Formerly ADM-23)		Lead Department: Administration	
Policy/Procedure Title: Conflict of Interest Code		☒ **External Policy** ☒ **Internal Policy**	
Original Date: 03/12/2010		**Next Review Date: 02/16/202402/15/2025** **Last Review Date: 02/16/202302/15/2024**	
Applies to:	☐ **Medi-Cal**	☐ **Healthy Kids**	☐ **Employees**

VI. POLICY / PROCEDURE:

A. Policy.

1. All PHC Board Members and internal PHC positions that make or influence decisions that may foreseeably have a material effect on PHC's economic interests, are considered designated positions, and shall file statements of economic interests, also known as the Form 700, pursuant with the information required for the disclosure category assigned to them and specified in Exhibit "A". Statements shall be filed annually, when an official assumes office, and when an official leaves office. Designated positions within PHC listed in Exhibit "B" are identified as Managers, Senior Managers, Associate Directors, Directors, Senior Directors, and C-level staff.

B. Procedure.

1. Assuming Office
   a. New Hires/New Board Members
      1) New hires holding a designated position as cited in Exhibit B, and new members to the PHC Board will have a profile created on the FPPC eDisclosure Portal, and within 30 days of assuming office, shall file their Form 700 electronically through the FPPC eDisclosure Portal.
   b. Existing Staff Transferring Positions
      1) Staff who transfer from a non-designated position to a designated position will have a profile created on the FPPC eDisclosure Portal and within 30 days of the official start date of the designated position, shall file their Form 700 electronically through the FPPC eDisclosure Portal.
      2) Existing online profiles for staff who transfer from one designated position to another will be updated to reflect the title and start ~~fate~~ date of the transferred position. However, the staff is not required to file a Form 700 until the next annual filing date.
2. Leaving Office
   a. Termed Employees
      1) Employees holding a designated position as cited in Exhibit B, who leave PHC will have their online profile updated with an end date reflecting when the employee officially left office. Prior to the official end date at PHC, but no later than 30 days post the end date, employees , shall file a Form 700 through the FPPC eDisclosure Portal.
   b. Board Members
      1) The PHC Board Clerk is responsible for updating a PHC Board Member's online profile when a board member leaves office and shall, list the last board meeting attended as the member's end date. No later than 30 days from the date of attendance at their final Board Meeting, Board Members will be required to file a Form 700 through the FPPC eDisclosure Portal
3. Amending the Code
   a. The Conflict of Interest Code may be amended at any time. Amendments are to be made by the Regulatory Affairs & Compliance (RAC) Unit, and will be forwarded to FPPC for review. When proposed amendments receive FPPC approval, RAC shall provide a Notice of Intention to Amend to staff, listing the changes that were made to the Code, and a 45-day written comment period will commence.
   b. During the 45-day written comment period, any interested person may submit comments relating to the proposed amendment by submitting them to RAC_Inbox@partnershiphp.org no later than the end of the written comment period, or at the conclusion of the public hearing, if requested. A person may request a public hearing no later than 15-days before

the close of the written comment period.

c. After the 45-day written comment period and/or after the public hearing, PHC's Chief Executive Officer (CEO) will sign a declaration stating the agency has satisfied all requirements preliminary to approval of the proposed Code. FPPC will finalize the Conflict of Interest Code upon receipt of the CEO's declaration.

VII. REFERENCES:

A. Board Resolution: 9.5 on January 26. 2011.

VIII. DISTRIBUTION:

A. PowerDMS
B. Directors

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE:

Compliance Officer

X. REVISION DATES:

1/31/11, 12/06/11, 12/04/12, 09/07/16, 08/16/2017, 02/22/2018, 05/24/2018, 05/16/2019, 11/19/2020, 02/17/2022, 02/16/2023, 02/15/2024

PREVIOUSLY APPLIED TO:

N/A

Policy/Procedure Number: CMP-21 (Formerly ADM-23)		Lead Department: Administration	
Policy/Procedure Title: Conflict of Interest Code – Attachment A		☒External Policy ☒Internal Policy	
Original Date: 03/12/2010		**Next Review Date:** ~~02/17/2023~~ 02/15/2025 **Last Review Date:** ~~02/17/2022~~ 02/15/2024	
Applies to:	☒ Medi-Cal	☐ Healthy Kids	☒ Employees

EXHIBIT A: CONFLICT OF INTEREST DISCLOSURE CATEGORIES

I. PLACE OF FILING OF STATEMENTS OF ECONOMIC INTERESTS

At the time of assuming office, annually thereafter, and upon leaving office, ~~I~~individuals holding designated positions with Partnership HealthPlan of California shall disclose and file statements of economic interests ~~with Partnership HealthPlan of California, which will make the statements available for public inspection and reproduction. (Gov. Code Sec. 81008.)~~ via mechanisms prescribed by the Fair Political Practice Commission (FPPC), as such, shall file their statement of economic interests (Form 700) electronically through the FPPC eDisclosure Portal. ~~Upon receipt of the statements, Partnership HealthPlan of California shall make and retain copies and forward the originals of these statements to the Fair Political Practices Commission.~~ All original statements shall be retained by the Fair Political Practices Commission.

II. DISCLOSURE CATEGORIES (REFER TO EXHIBIT "A")

The categories listed in Exhibit "A" provides the type of personal interest that must be disclosed on the Statements of Economic Interests (Form 700).

III. DESIGNATED POSITIONS (REFER TO EXHIBIT "B")

Persons holding designated positions listed in Exhibit "B" shall file Statements of Economic Interests pursuant to §5 of the Model Code with the information required for the disclosure category assigned to them and specified in Exhibit "A".

IV. Addendum to Conflict of Interest Code

Gifts: Pursuant to Government Code Section 89503(c) and Title 2, California Code of Regulations Section 18730(b)(8.1), designated employees pursuant to the Conflict of Interest Code of Partnership HealthPlan of California may not accept gifts with a total value of more than five hundred dollars ($500) in a calendar year from any single source, if the employee would be required to report the receipt of such income or gifts from that source on his or her statement of economic interests. The $500 threshold is updated annually by the Fair Political Practices Commission to reflect changes in the Consumer Price Index, rounded to the nearest ten dollars ($10). (Government Code Section 89503(f)).

Honoraria: Pursuant to Government Code Section 89502(c), no designated employee of Partnership HealthPlan of California may accept an honorarium from any source if the employee would be required to report the receipt of income or gifts from that source on his or her statement of economic interests.

Policy/Procedure Number: CMP-21 (Formerly ADM-23)		Lead Department: Administration	
Policy/Procedure Title: Conflict of Interest Code – Attachment A		☒External Policy ☒Internal Policy	
Original Date: 03/12/2010		**Next Review Date:** ~~02/17/2023~~ 02/15/2025 **Last Review Date:** ~~02/17/2022~~ 02/15/2024	
Applies to:	☒ Medi-Cal	☐ Healthy Kids	☒ Employees

DISCLOSURE CATEGORIES

Category 1
Interests in real property within 2,000 feet from property owned or used by Partnership HealthPlan of California or that may be acquired by the Partnership HealthPlan of California for its use.

Category 2
Investments, business positions in business entities and income (including receipt of gifts, loans and travel payments) from sources of the type to provide:

- Medical/health care treatment, facilities, services, products, equipment, machines,
- Medical insurance products and services and,
- Other products and services utilized by the District including telecommunications and information technology, janitorial, and legal.

The medical/health care sources include the full range of products and services including: medical providers, hospitals, pharmaceutical products/facilities, transportation companies and consultants.

Category 3
Investments, business positions, and sources of income (including receipt of loans, gifts, and travel payments) from sources that provide, or have provided, services, supplies, materials, machinery, or equipment of the type utilized by the designated position's department or division.

Category 4
Investments and business positions in business entities and sources of income (including receipt of loans, gifts, and travel payments) that have filed a claim or have a claim pending against Partnership HealthPlan of California.

Policy/Procedure Number: CMP-21 (Formerly ADM-23)		Lead Department: Administration	
Policy/Procedure Title: Conflict of Interest Code – Attachment B		☒External Policy ☒Internal Policy	
Original Date: 03/12/2010		**Next Review Date:** ~~02/17/2023~~02/15/2025 **Last Review Date:** ~~02/17/2022~~ 02/15/2024	
Applies to:	☐ Medi-Cal	☐ Healthy Kids	☒ Employees

EXHIBIT B: CONFLICT OF INTEREST DESIGNATED POSITIONS

Designated Positions	Disclosure Categories
Chief Executive Officer	1,2
Chief Information Officer	1,2
Chief Medical Officer	1,2
Chief Operating Officer/ Deputy CEO	1,2
Chief Strategy and Government Affairs Officer	1,2
Board Members	1,2
Consultants/ New Positions	*
Senior Directors	2
Executive Director	2
Directors	2
Director of Claims	2,4
Director of Configuration	2,4
Medical Director	2
Regional Director	3
Behavioral Health Administrator	2
Associate Directors *(Except Associate Directors of Claims Operation and Associate Director of Configuration)*	3
Associate Director of Claims Operation	3,4
Associate Director of Configuration	3,4
Senior Managers	3
Managers *(Except Claims Manager, Claims Configuration Manager, Claims Customer Service Manager)*	3
Manager of Claims	4
Manager of Configuration	4
Manager of Claims Customer Service	4
Team Manager	3
~~Program Managers II~~	~~3~~

*Consultants/New Positions shall be included in the list of designated positions and shall disclose pursuant to the broadest disclosure category in the code subject to the following limitations:

The Chief Executive Officer may determine in writing that a particular consultant/new position, although a "designated position," is hired to perform a range of duties that are limited in scope and thus is not required to fully comply with the disclosure requirements described in this section. Such written determination shall include a description of the consultant's/new position's duties and, based on that description, a statement of the extent of the disclosure requirements. The Chief Executive Officer's determination is a public record and shall be retained for public inspection in the same manner and location as this conflict of interest code (Government Code Sec. 81008)

OFFICIALS WHO MANAGE PUBLIC INVESMENTS

Policy/Procedure Number: CMP-21 (Formerly ADM-23)		Lead Department: Administration	
Policy/Procedure Title: Conflict of Interest Code – Attachment B		☒**External Policy** ☒**Internal Policy**	
Original Date: 03/12/2010		**Next Review Date:** ~~02/17/2023~~02/15/2025 **Last Review Date:** ~~02/17/2022~~ 02/15/2024	
Applies to:	☐ **Medi-Cal**	☐ **Healthy Kids**	☒ **Employees**

The following positions are NOT covered by the conflict-of-interest code because they must file under Government Code Section 87200 and, therefore, are listed for informational purposes only:

- Controller/Senior Director of Accounting
- Chief Financial Officer

An individual holding one of the above-listed positions may contact the Fair Political Practices Commission for assistance or written advice regarding their filing obligations if they believe that their position has been categorized incorrectly. The Fair Political Practices Commission makes the final determination whether a position is covered by Government Code Section 87200.

DHCS All Plan Letter APL 23-031
Adult Expansion Transition 26-49

Impacted Departments: MS, UM, CC, PR, Configuration, IT, QI, BH, PH

CC: APL Distribution List

From: Regulatory Affairs/Compliance (RAC) – Danielle Dillard

Date: 12/21/2023

RE: Adult Expansion Transition 26-49

Purpose:
Guidance on the Age 26-49 Adult Expansion to ensure individuals transitioning from restricted scope Medi-Cal or are otherwise uninsured to full-scope Medi-Cal maintain their existing Primary Care Provider (PCP) assignments to the maximum extent possible to minimize disruptions in services.

PCPs include:

- general practitioner
- internist
- pediatrician
- family practitioner
- non-physician medical practitioner
- obstetrician-gynecologist
- specialists
- medical homes
- clinics

MCPs must coordinate with county uninsured programs and public health care systems to share data for the Adult Expansion Population and use that data to effectuate PCP assignment.

Highlights:

- Much of the Adult Expansion Population is currently served through county programs for the uninsured and low-income populations and public health care systems. As these individuals transition to full scope Medi-Cal, California has prioritized two goals:
    - Maintain PCP assignment to the maximum extent possible
    - Support and strengthen traditional county health providers who treat a high volume of uninsured and Medi-Cal patients.

Impacted Populations

- New Enrollee Population
    - The new enrollee population consists of individuals who are 26 through 49 years of age in January 2024, who are not currently enrolled in full scope or restricted scope Medi-Cal, but who

may apply for Medi-Cal after implementation of the Age 26-49 Adult Expansion and meet all eligibility criteria for full scope Medi-Cal, under any eligibility group, including Modified Adjusted Gross Income (MAGI) and Non-MAGI, except for SIS.

- Transition Population
  - The transition population consists of individuals who are 26 through 49 years of age and are currently enrolled in restricted scope Medi-Cal because they do not have SIS or are unable to establish SIS for full scope Medi-Cal under any eligibility group, including MAGI and Non-MAGI, before implementation of this expansion.
- New Enrollee Populations and Transition Populations will be considered “Adult Expansion Populations”

Data Sharing and Coordination Policy

- DHCS is requiring MCPs to effectuate a data sharing process with the county uninsured programs and public health care systems that currently serve the Adult Expansion Population. MCPs are required to accept data from, transmit data to, and coordinate with, the county uninsured programs and public health care systems serving the Adult Expansion Population.

Data Sharing Authority and Regulations

- Covered entities are permitted to share health care data with other covered entities for treatment, payment, or healthcare operations purposes.
- DHCS requires MCPs to coordinate with healthcare providers and county uninsured programs as part of their obligations to coordinate services.

Data Sharing Process

- MCPs will receive the Member PCP Assignment File from the county uninsured program or the public health care system, review the data file, and use the data elements provided to complete a Member match and PCP assignment.
- The MCP must send back the PCP Assignment Return File confirming which Members were successfully assigned a PCP match.
- MCPs must ensure compliance with the HIPAA privacy and security rules. MCPs must establish process and procedures to securely destroy data for individuals who do not ultimately enroll into the MCP in compliance with HIPAA regulations.

Matching Policy

- MCPs should develop matching processes to identify unique individuals in the county uninsured programs or public health care systems, for example by using data elements such as name, date of birth, and address.

Continuity of Care and Assignment Policy

- Member choice of PCP is paramount and must be prioritized over any auto-assignment processes.
- For Adult Expansion Population Members with an existing PCP that is in-Network with the receiving MCP, the MCP is required to maintain that assignment.

- Adult Expansion Population Members are not required to request continuity of care to maintain their PCP assignment With PCPs that are in the MCP's Network.

Timing

- MCPs must begin accepting data from county uninsured programs and public health care systems immediately upon the publishing of this APL, and continue accepting data through June 30, 2024, as necessary to effectuate assignment.

Expectations

- If the MCP does not have an executed contract with the assigned PCP effective before June 30, 2024, the MCP is not required to effectuate the PCP assignment, but must offer continuity of care for provider agreement if all continuity of care for provider agreement requirements are met per APL 23-022.

Assessment of Compliance

- DHCS will assess MCPs' compliance with the requirements laid forth in this APL via post transitional monitoring, coordination with county uninsured programs and public health care systems and other stakeholders, and reviews of regular MCP reporting streams including but not limited to the Primary Care Physician Assignment File.
- MCP is responsible for and must have mechanisms to ensure that subcontractors/delegates maintain compliance with requirements of the APL.

ACTION REQUIRED:

Please provide a response to the Regulatory Guidance inbox by March 12, 2024.

DHCS All Plan Letter APL 23-032

ECM Requirements

Impacted Departments: CC, MS, PH, UM

CC: APL Distribution List

From: Regulatory Affairs/Compliance (RAC)

Date: 12/22/2023

RE: ECM Requirements

Purpose: Provide guidance to all Medi-Cal managed care plans (MCPs) regarding the provision of the Enhanced Care Management (ECM) benefit.

Highlights:

- Effective upon the DHCS determined ECM implementation date for each MCP in its respective county of operation, the MCP must administer ECM and provide the following seven core ECM services to eligible Members in applicable ECM Populations of Focus:
  - Outreach and Engagement
    - The MCP is responsible for reaching out to and engaging Members who are identified to be eligible for ECM.
  - Comprehensive Assessment and Care Management Plan
    - Engaging with each Member authorized to receive ECM,
    - Identifying necessary clinical and non-clinical resources
    - Developing a comprehensive, individualized, person-centered Care Management Plan
    - Incorporating into the Member's Care Management Plan identified needs and strategies to address those needs
    - Ensuring the Member is reassessed at a frequency appropriate for the Member's individual progress, changes in needs, and/or as identified in the Care Management Plan
    - Ensuring the Care Management Plan is reviewed, maintained, and updated under appropriate clinical oversight.
  - Enhanced Coordination of Care
    - Organizing patient care activities, as laid out in the Care Management Plan
    - Maintaining regular contact with all Providers that are identified as being a part of the Member's multi-disciplinary care team
    - Ensuring care is continuous and integrated among all service Providers
    - Providing support to engage the Member in their treatment
    - Communicating the Member's needs and preferences timely to the Member's multi-disciplinary care team
    - Ensuring regular contact with the Member and their family members, legal guardians, authorized representatives, caregivers, and authorized support persons, as appropriate, consistent with the Care Management Plan.

- Health Promotion
  - Working with the Member to identify and build on successes and potential family and/or support networks
  - Providing services to encourage and support the Member to make lifestyle choices based on healthy behavior
  - Supporting the Member in strengthening skills
- Comprehensive Transitional Care
  - Developing strategies to reduce avoidable Member admissions and readmissions across all Members receiving ECM
  - Providing assistance to members who are experiencing or are likely to experience a care transition
- Member and Family Supports
  - Documenting the member's authorized caregivers and care team
  - Ensuring all required authorizations are in place
  - Activities to ensure member's authorized caregivers and care team are knowledgeable about the member's conditions
  - Ensuring the Member's ECM Lead Care Manager serves as the primary point of contact
  - Identifying supports needed for the Member and the members authorized caregivers and care team
  - Providing appropriate education
  - Provide a copy of the Member's Care Management Plan and information about how to request updates.
- Coordination of and Referral to Community and Social Support Services.
  - Determining appropriate services to meet the needs of the Member, including services that address social determinants of health needs, such as housing, and services offered by the MCP as ILOS
  - Coordinating and referring the Member to available community resources and following up with the Member to ensure services were rendered (i.e., "closed loop referrals").

Additional Guidance:

- ECM Populations of Focus (POF):
  - MCPs must proactively identify and offer ECM to their high-need, high-cost Members who meet the POF criteria listed in the Contract and detailed in Attachment 1 of this APL.
- ECM Provider Standard Terms Conditions (STCs):
  - MCPs must ensure ECM is provided primarily through in-person interaction
- ECM Model of Care (MOC):
  - MCPs must develop and submit to DHCS for review and approval an ECM MOC.
  - MCPs must submit to DHCS any significant updates to their MOCs for DHCS review and approval at least 60 calendar days in advance of significant changes or updates.
- ECM Encounter Data Reporting:
  - MCPs must report all ECM encounters to DHCS, using the defined set of ECM Healthcare Common Procedure Coding System codes and modifiers.
- ECM Policy Guide:
  - The ECM Policy Guide outlines ECM policies and contains details of MCPs' contractual requirements for ECM. The ECM Policy Guide includes operational guidelines, including reporting requirements for ECM. MCPs must use the ECM Policy Guide as a key resource for implementation and administration of ECM.

ECM Rates

- For the Calendar Year (CY) 2022, 2023 and 2024 rating periods, a two-sided, symmetrical risk corridor is in effect for applicable revenues and expenditures associated with ECM, as determined by DHCS.

MCP is responsible for and must have mechanisms to ensure that subcontractors/delegates maintain compliance with requirements of the APL.

ACTIONS:
Please provide a P&P or a completed internal checklist (if no P&P updates are needed) to Regulatory Guidance by March 14, 2024

DHCS All Plan Letter APL 23-034
California CCS WCM Program

Impacted Departments: Care Coordination, Utilization Management, Pharmacy, Claims, Quality Improvement

CC: APL Distribution List

From: Regulatory Affairs/Compliance (RAC) - Lonni Hemphill

Date: 12/28/2023

RE: California CCS WCM Program

Purpose: Provide guidance to MCPs participating in the California Children's Services (CCS) Whole Child Model (WCM) Program. [*Supersedes APL 21-005*]

Highlights of requirements:(*consistent with those previously states in APL 21-005 with the following changes***)**:

The WCM Program has been implemented and various counties (see enclosed breakdown with MCP assignment) and will be effective January 1, 2024 and January 1, 2025.

MCPs must:

- Provide documentation (medical records, case notes, reports related to CCS eligible condition) to the County CCS Program for initial / annual medical eligibility determines
- Must refer a member to the county for a CCS eligibility determination
- Required to provide services to CCS eligible members with other health coverage, with full scope Medi-Cal as the payor of last resort
- Must review offered coverages to prevent duplication of services
- Must review MOUs annually to determine if any modifications of responsibilities are needed
- Designate at least one individual as the primary point of contact (POC) responsible for CCS members' care coordination
  - Individual must be knowledgeable of / receive adequate training on the CCS Program
  - Have clinical experience with either the CCS population or pediatric patients with complex medical conditions
  - Must receive training on full spectrum of rules and regulation for CCS
  - Liaison can also be POC for ECM and CS providers that serve CCS eligible members under the ECM populations of focus
- Must review and complete Inter-County Transfer (ICT) requests
  - Plans must collaborate with receiving counties on their negotiations with the previous counties of a transfer date and open the case

  - When counties cannot come to an agree on the transfer process, the county or MCP should contact DHCS for assistance (CCSProgram@dhcs.ca.gov)
- Must refer potential NICU and HRIF cases to the County CCS Program
- Must carry out all responsibilities under the MOU without delay (including providing members with access to services under the MOU) during a dispute between MCP and County CCS Program
- Must have a formal process to accept, acknowledge and resolve provider disputes and grievances
- Must refer all members who may have developed a new CCS-eligible condition as soon as possible to County CCS with appropriate documentation
- Must establish an ICP for all members determined to be high risk based on the risk assessment process within 12 months
  - ICP members determined to be high risk must be established within 90 calendar days of a completed risk assessment survey or other assessment
    - If ICP is declined by family, the MCP must notate the denial in the member's medical record as evidence of compliance
- Must allow members to access CCS Paneled providers within all of the MCP's subcontracted provider network for CCS services
- Required to cover all medically necessary blood, tissue, and solid organ transplants for CCS eligible members
- Must reimburse member/family for paid M&T expenses no later than 60 calendar days following confirmation that all required receipts/documentation have been received
- Plan representatives must meet quarterly with the WCM Program stakeholder advisory group composed of representatives of CCS provider, County CCS Program administrators, health plans, family resource centers, regional centers, recognized exclusive representatives of County CCS providers, CCS case managers, CCS MTUs, and representatives from Family Advisory Committees

MCP-to-MCP member transitions prompted by changes to commercial MCP contracting or an Alternate Health Care Service Plan (AHCSP) contract with Kaiser must adhere to all requirements of the 2024 MCP Transition Policy Guide.

ECM can be provided to members in addition to the WCM Program, as long as services are not duplicative.

Reimbursements for M&T expenses are available to the CCS-eligible member/family in accordance with CCS N.L. 03-0810

ACTIONS: within 90 days from the release of the APL, PHC must submit an attestation of no impact or a revised policy to address APL requirements. Please submit P&P's to Regulatory Guidance by **March 19, 2024**.

DHCS All Plan Letter APL 23-035

Student Behavioral Health Incentive Program (SBHIP)

Impacted Departments: Configuration, Finance, QI, BH

CC: APL Distribution List

From: Regulatory Affairs/Compliance (RAC) – Danielle Dillard

Date: 01/02/2024

RE: Student Behavioral Health Incentive Program (SBHIP)

Purpose: Provide Medi-Cal managed care plans (MCPs) with guidance on the incentive payments provided by the Student Behavioral Health Incentive Program (SBHIP). SBHIP is a part of California's Children and Youth Behavioral Health Initiative (CYBHI) and is being implemented by the Department of Health Care Services (DHCS)

Highlights of requirements*:*

- Please see draft APL for SBHIP Deliverable Submission Timeline.
- The objectives of SBHIP are to:
    - Break down silos and improve coordination of child and adolescent student behavioral health services through increased communication with schools, school-affiliated programs, managed care Providers, counties, and mental health providers.
    - Increase the number of TK-12 students enrolled in Medi-Cal receiving behavioral health services through schools, school-affiliated providers, County Behavioral Health Departments, and County Offices of Education (COEs).
    - Increase non-specialty services on or near school campuses.
    - Address health equity gaps, inequalities, and disparities in access to behavioral health services.

Policy: Incentive payments provided through SBHIP must supplement and not supplant existing payments to MCPs.

MCP Eligibility and Participation:

- MCP participation in this incentive program is voluntary, but strongly encouraged.
- MCPs are also encouraged, but not required, to partner with County Behavioral Health Departments.

MCP Incentive Payments:

- DHCS is allocating $389 million in SBHIP incentive payments to MCPs over a three-year period (January 1, 2022 - December 31, 2024).
- SBHIP incentive payments are divided between two funding allocations: Needs Assessment allocations and Targeted Intervention allocations.

  - Total Needs Assessment Allocations Available: Approximately $39 million
  - Total Targeted Intervention Allocations Available: Approximately $350 million
- Please see Table 2 for SBHIP Funding Allocation Milestones and Distribution Dates.

Requirements for Needs Assessment Funds:

- To be eligible to receive full Needs Assessment funding, MCPs were required to demonstrate partnership with a minimum of ten percent of the LEAs in a county to conduct the Needs Assessment.
- MCPs were required to report LEA partners on both the Partners Form and in the Needs Assessment.

Requirements for Targeted Intervention Funds:

- MCPs are required to implement a minimum number of Targeted Interventions, dependent upon their county's Targeted Intervention allocation.
- Please see Table 3 for the Minimum Targeted Intervention Assignment Methodology.
- Please see Table 4 for the Targeted Intervention Funding Allocation Parameters

Targeted Interventions:

- MCPs may select from the following 14 SBHIP Targeted Intervention categories:
  - Behavioral Health Wellness Programs
  - Telehealth Infrastructure to Enable Services and/or Access to Technological Equipment
  - Behavioral Health Screenings and Referrals
  - Suicide Prevention Strategies
  - Substance Use Disorder
  - Building Stronger Partnerships to Increase Access to Medi-Cal Services
  - Culturally Appropriate and Targeted Populations
  - Behavioral Health Public Dashboards and Reporting
  - Technical Assistance Support for Contracts
  - Expand Behavioral Health Workforce
  - Care Teams
  - Information Technology (IT) Enhancements for Behavioral Health Services
  - Pregnant Students and Teen Parents
  - Parenting and Family Services
- MCPs are expected to work with COEs and LEAs to implement the Targeted Interventions and encouraged to continue collaborating post-implementation. When partnering, MCPs must develop MOUs for:
  - Partnerships between MCPs, COEs, and LEAs
  - MCPs collaborating with other MCPs to implement SBHIP Targeted Interventions within a county

Program Measurement:

- Performance in SBHIP is measured in two ways:
  - Deliverable Scoring
    - Deliverable Scoring evaluates and scores four deliverables:
      - Needs Assessment
      - Project Plans (Milestone One)
      - Bi-Quarterly Reports
      - Project Outcome Reports (Milestone Two)
    - Please see Table 5 for the Deliverable Scoring and Evaluation Criteria
    - Deliverable scores determine whether an MCP will receive Needs Assessment or Targeted Intervention allocations.
      - Please see Table 6 for SBHIP Deliverable Payment Thresholds
  - Performance Outcome Metrics.
    - MCPs will be required to select one of two Performance Outcome Metrics for each Targeted Intervention. Performance Outcome Metrics include:
      - Performance Outcome Metric #1: Increase access to behavioral health services (capacity, infrastructure, sustainability, behavioral health service) for Medi-Cal Members on or near campus
      - Performance Outcome Metric #2: Increase access to behavioral health services (capacity, infrastructure, sustainability, behavioral health service) for Medi-Cal Members provided by school-affiliated behavioral health providers
    - Examples of Performance Measures may include but are not limited to:
      - Number of students attending a suicide prevention program
      - Number of behavioral health Telehealth services provided
      - Number of behavioral health providers
      - Number of Care Team members
      - Number of behavioral health staff trainings
      - Number of students attending behavioral health trainings
      - Frequency of behavioral health presentations, and
      - Number of Behavioral Health Wellness rooms

Calendar Year 2024 Transition:

- MCPs, including all who are participating in SBHIP will be required to develop a plan for the transition of SBHIP responsibilities to ensure the continuity and success of the program in their respective county.
- The Transition Plan consists of two separate deliverables and should be completed in collaboration with all of the participating Medi-Cal MCPs in a county.
  - Transition Plan Part 1 (Due June 30, 2023)
  - Transition Plan Part 2 (Due September 29, 2023)
- If, in a county, there are no remaining MCPs and only one incoming MCP, then the exiting MCP's CY 2024 funding will be re-allocated fully to the sole incoming MCP. If there are multiple remaining and/or incoming MCPs in a county, then the exiting MCP's CY 2024 funding will be re-allocated amongst the

MCPs and will be based upon the percentage of the exiting MCP's CY 2024 membership assumed by the remaining and/or incoming MCP(s).

- In Quarter 1 of CY 2024, DHCS will provide remaining and/or incoming MCPs with preliminary payment amounts based on estimated enrollment. MCP's CY 2024 funding amounts will be finalized in Quarter 2.

DHCS Program Oversight:

- DHCS will monitor the timeliness of MCP submissions, as well as the content of the deliverables, and request revisions for incomplete submissions, as needed.
- MCPs must review their contractually required policies and procedures (P&Ps) to determine if amendments are needed to comply with this APL.

ACTIONS:

- Please provide a P&P or a completed internal checklist (if no P&P updates are needed) to the Regulatory Guidance inbox **by March 20, 2024**.

DHCS All Plan Letter 24-001

Street Medicine Provider: Definitions and Participation in Managed Care

Impacted Departments: UM, CC, PH, BH, PR, Finance

CC: APL Distribution List

From: Regulatory Affairs/Compliance (RAC)

Date: January 16, 2024

RE: Street Medicine Provider: Definitions and Participation in Managed Care

Purpose: Provide guidance to Medi-Cal managed care plans (MCPs) on opportunities to utilize street medicine providers to address clinical and non-clinical needs of their Medi-Cal Members experiencing unsheltered homelessness. (*Supersedes APL 22-023)*

Highlights:

Definition:

- Street Medicine: set of health and social services developed specifically to address the unique needs and circumstances of individuals experiencing unsheltered homelessness, delivered directly to them in their own environment.
- Brick-and-Mortar: primary care medical office, Federally Qualified Health Center (FQHC), clinic, etc.

Policy:

MCPs may cover the provision of medical services for their Members experiencing unsheltered homelessness through street medicine providers in the role of the Member's assigned PCP, through a direct contract with the MCP, as an ECM Provider, as a Community Supports Provider, or as a referring or treating contracted Provider.

Street Medicine Provider as a Member's Assigned PCP:

- Street medicine provider
  - Licensed medical provider
    - Doctor of Medicine (MD)/Doctor of Osteopathic Medicine (DO)
    - Physician Assistant (PA)
    - Nurse Practitioner (NP)
    - Certified Nurse Midwife (CNM)
- Non-physician medical practitioner (PA, NP, CNM)
  - MCPs must ensure compliance with state law and Contract requirements regarding physician supervision of non-physician medical practitioners.

- Street medicine Providers who choose to act as a Member's assigned PCP must agree to provide the essential components of the Medical Home in order to provide comprehensive and continuous medical care, including but not limited to:
  - Basic Population Health Management
  - Care coordination and health promotion
  - Support for Members, their families, and their authorized representatives;
  - Referral to Specialists, including behavioral health, community, and social support services, when needed
  - The use of Health Information Technology to link services, as feasible and appropriate
  - Provision of primary and preventative services to assigned Members.

Site Review and Medical Record Review Requirements:

- Street medicine Providers who are serving in an assigned PCP capacity are required to undergo the appropriate level of site review process, which is either a full or a condensed review.
  - For street medicine Providers serving as an assigned PCP, and that are affiliated with a brick-and-mortar facility or that operate a mobile unit/RV, the MCP must conduct the full review process of the street medicine Provider and affiliated facility in accordance with APL 22-017: Primary Care Provider Site Reviews: Facility Site Review and Medical Record Review.
  - For street medicine, Providers serving as an assigned PCP, and that are not affiliated with a brick-and-mortar facility or mobile unit/RV, the MCP must conduct a condensed Facility Site Review (FSR) and Medical Record Review (MRR) of the street medicine Provider to ensure Member safety.

Process for Street Medicine Provider to Become Member's Assigned PCP:

- If an MCP has street medicine Providers willing to serve in a PCP capacity, MCPs must inform Members through the Member Handbook that contracted street medicine Providers may be elected to be the Member's assigned PCP so that the Member and the street medicine Provider can discuss whether this arrangement is appropriate.
- Street medicine Providers are advised to assess and examine the level and quality of the establishment of the treatment relationship at the time of initial engagement when considering an agreement to be a Member's assigned PCP, as DHCS envisions dynamic and exceptional Provider-Member patient interactions.
- DHCS encourages MCPs to establish a streamlined PCP assignment process for street medicine Providers.

Provider Enrollment and Credentialing:

- Criteria that MCPs may want to consider as part of their vetting processes include, but is not limited to:
  - Sufficient experience providing similar services within the service area
  - Ability to submit claims or invoices using standardized protocols
  - Business licensing that meets industry standards
  - Capability to comply with all reporting and oversight requirements
  - History of fraud, waste, and/or abuse

- Recent history of criminal activity, including a history of criminal activities that endanger Members and/or their families
- History of liability claims against the provider.

Access Requirements:

Street medicine Providers elected as a Member's assigned PCP are exempt from PCP time and distance standards as the Member does not have a permanent residential address and the street medicine Provider is meeting the Member at their lived environment.

Direct Contracting Arrangement

- DHCS encourages MCPs to contract directly with street medicine Providers. Even if the MCP delegates the provision of health care services to a Subcontractor, MCPs have an option to directly contract with street medicine Providers.

Street Medicine Provider as an ECM Provider

- MCPs may contract with street medicine Providers to become an ECM Provider. A street medicine Provider can be contracted to provide both PCP and ECM services to a Member.

Street Medicine Providers Serving Solely as Referring or Treating Contracted Provider

- To provide care in this capacity, street medicine Providers must have processes in place to work with the MCP, the Member's PCP, and ECM Care Manager to ensure the Member has referrals to primary care, Community Supports, behavioral health services, and other social services as needed.

Medi-Cal Eligibility

- Medi-Cal eligible individuals will be covered by either the Medi-Cal Fee-for-Service (FFS) or Medi-Cal managed care (with a corresponding MCP) delivery system.
- Individuals without Medi-Cal coverage, the Hospital Presumptive Eligibility (HPE) program is one pathway for qualified HPE Providers to determine Medi-Cal eligibility. HPE provides qualified individuals immediate access to temporary Medi-Cal services while individuals apply for permanent Medi-Cal coverage.

Billing/Reimbursement

- Street medicine Providers must comply with the billing provisions for street medicine Providers as applicable in FFS, including but not limited to, the Medi-Cal Provider Manual.
- The Centers for Medicare and Medicaid Services (CMS) created a new Place of Service (POS) code 27 (Outreach Site/Street) that became effective October 1, 2023. Street medicine providers should bill POS code 27 to Medi-Cal FFS or MCPs when rendering services for street medicine, as defined in this APL, as of October 1, 2023.
- POS codes 04 (Homeless Shelter), 15 (Mobile Unit), and 16 (Temporary Lodging) should continue to be utilized for services provided in those respective settings. DHCS would like to reiterate that both street medicine and mobile medicine are reimbursable services in accordance with billing protocols and a provider's scope of practice; however, it remains the expectation of DHCS that individuals experiencing

unsheltered homelessness receive appropriate and applicable services in their lived environment via street medicine.

Data Sharing, Reporting and Administration Requirements

- MCPs are to ensure street medicine Providers receive appropriate provider training and manuals, and have adequate systems in place to adhere to data sharing and reporting requirements, such as for encounter, claims, and care coordination data.
- MCPs must review their contractually required policies and procedures (P&Ps) to determine if amendments are needed to comply with this APL.
- MCP is responsible for and must have mechanisms to ensure that subcontractors/delegates maintain compliance with requirements of the APL.
- DHCS may impose Corrective Action Plans (CAP), as well as administrative and/or monetary sanctions for non-compliance. For additional information regarding administrative and monetary sanctions, see APL 23-012, and any subsequent iterations on this topic. Any failure to meet the requirements of this APL may result in a CAP and subsequent sanctions.

Actions:

- Please provide a P&P or a completed internal checklist (if no P&P updates are needed) to Regulatory Guidance by **April 4, 2024**.

DHCS All Plan Letter APL 24-002 MCP Responsibilities IHCP

Impacted Departments: IHS, CC, UM, Transportation, PR, Claims, MS

CC: APL Distribution List

From: Regulatory Affairs/Compliance (RAC)

Date: Thursday, February 8, 2024

RE: MCP Responsibilities IHCP

Purpose:
Summarize and clarify existing federal and state protections and alternative health coverage options for American Indian Members enrolled in Medi-Cal managed care plans (MCPs). Additionally, this APL consolidates various MCP requirements pertaining to protections for Indian Health Care Providers (IHCPs), including requirements related to contracting with IHCPs and reimbursing claims from IHCPs in a timely and expeditious manner. This APL also provides guidance regarding MCP tribal liaison requirements and expectations in relation to their role and responsibilities.

Supersedes APL 09-009

Highlights:

Definitions:

- Federal law defines an individual as an "Indian" if the individual meets any of the following criteria:
  - Is a member of a Federally recognized Indian tribe
  - Resides in an urban center and meets one or more of the four following criteria:
    - Is a member of a tribe, band, or other organized group of Indians, including those tribes, bands, or groups terminated since 1940 and those recognized now or in the future by the State in which they reside, or who is a descendant, in the first or second degree, of any such member
    - Is an Eskimo or Aleut or other Alaska Native
    - Is considered by the Secretary of the Interior to be an Indian for any purpose
    - Is determined to be an Indian under regulations issued by the Secretary of Health and Human Services.
  - Is considered by the Secretary of the Interior to be an Indian for any purpose
  - Is considered by the Secretary of Health and Human Services to be an Indian for purposes of eligibility for Indian health care services, including as a California Indian, Eskimo, Aleut, or other Alaska Native.

- The MCP Contract defines “American Indian” as a Member who meets the criteria for an “Indian” as defined in federal law. For consistency with the MCP Contract, this APL uses the term “American Indian.”
- Federal law defines an IHCP as a health care program operated by:
    - The Indian Health Service (IHS), which means the agency of that name within the U.S. Department of Health and Human Services established by the Indian Health Care Improvement Act (IHCIA) Section 601, 25 USC Section 1661;
    - An Indian Tribe, which has the meaning given in the IHCIA Section 4(14), 25 USC Section 1603(14);
    - A Tribal Organization, which has the meaning given in the IHCIA Section 4(25), 25 USC Section 1603(26);
    - An Urban Indian Organization (otherwise known as a UIO), which has the meaning given in the IHCIA Section 4(29), 25 USC Section 1603(29)
- Tribal Health Program means an American Indian tribe or tribal organization that operates any health program, service, function, activity, or facility funded, in whole or part, by the IHS through, or provided for in, a contract or compact with the IHS under the Indian Self-Determination and Education Assistance Act5 and is defined in 25 USC section 1603(25).

American Indian Member Rights and Protections:

- American Indian Medi-Cal Members are not required to enroll in an MCP, except in the case of County Organized Health Systems (COHS) or Single Plan Model counties.
- An American Indian MCP Member can request to receive services from an IHCP and can choose an IHCP within the MCP’s Network as a Primary Care Provider (PCP).
- When an American Indian MCP Member requests to receive services from an IHCP, and there is no in-network IHCP available, then the MCP must assist the Member in locating and connecting with an out-of-network IHCP.

IHCP Rights and Protections

- Existing rights and protections for IHCPs, on the topics of enrollment, contracting, credentialing and site review, and claims payment, are described below.
    - IHCP Enrollment
        - If an IHCP is providing Medi-Cal covered services, including transportation, to an American Indian MCP Member, the MCP must ensure that the IHCP is enrolled in the Medi-Cal program.
        - State-Level Enrollment Pathway
            - MCPs should be aware that IHCPs enrolling through the Medi-Cal FFS program are subject to DHCS’ rules, processing requirements, and enrollment time frames.

- DHCS is allowed up to 180 days to act on an enrollment application. If a case is referred or has been returned to a Provider for correction, a determination may not occur within 180 days.

- Ordering, Referring, and Prescribing Provider Enrollment
  - MCPs must ensure that individual practitioners who provide services at an IHCP facility are enrolled in Medi-Cal as an Ordering, Referring, and Prescribing (ORP) Provider.
  - MCP is prohibited from requiring the licensure of a health professional employed by a Tribal Health Program under the state or local law where the Tribal Health Program is located, if the professional is licensed in another state
- IHCP Contracting
  - To ensure proper and timely claims payment to IHCPs, DHCS reminds MCPs that IHCPs do not have to contract with an MCP as a Network Provider, nor do IHCPs have to contract with any MCP Subcontractor, in order to be reimbursed by either the MCP or the Subcontractor for services provided to an American Indian MCP Member.
  - Within 15 days of receiving a Network Provider application submitted by an IHCP, an MCP must provide acknowledgment of receipt in a written notice to the IHCP.
  - Other IHCP Contracting Requirements:
    - MCP contracts with IHCPs cannot be construed to in any way change, reduce, expand, or alter the eligibility requirements for services through the IHCP's programs, as determined by federal law.
    - IHCPs cannot be required to obtain or maintain insurance (including professional liability insurance), provide indemnification, or guarantee that the MCP will be held harmless from liability.
- IHCP Credentialing/Re-Credentialing and Site Reviews
  - MCPs are required to ensure that IHCPs contracting as Network Providers are properly credentialed and re-credentialed, in accordance with the MCP Contract29 and APL 22-013: Provider Credentialing/Re-Credentialing and Screening/Enrollment, or any subsequent updates.
- IHCP Claims Payment
  - Claims Payment Timeliness
    - IHCPs are entitled to timely and expeditious payment of claims in accordance with federal and state law and APL 23-020. The IHCP does not need to have a contract with an MCP in order to receive reimbursement for services provided to an American Indian MCP Member.
    - MCPs must reimburse IHCPs that provide Covered Services in a timely and expeditious manner. The federal standard is payment of 90 percent of all clean claims (i.e., claims that require no additional information) within 30 calendar days of receipt, and payment of 99 percent of all clean claims within 90 calendar days of receipt.

- Transportation Reimbursement
  - MCPs must reimburse IHCPs for transporting an American Indian MCP Member to an IHCP.
  - If an IHCP wishes to provide transportation services to non-American Indian MCP Members, the IHCP must be enrolled in the Medi-Cal program as a transportation provider and must contract with the MCP and/or the MCP's delegated transportation provider.

MCP Tribal Liaison

- Effective January 1, 2024, MCPs are required to have an identified tribal liaison dedicated to working with each contracted and non-contracted IHCP in its service area.
- Please see the APL for the role and responsibilities of the MCP tribal liaison.
- Please see the APL for a list of activities to enhance relationships between MCPs, IHCPs, and American Indian MCP Members.

MCP is responsible for and must have mechanisms to ensure that subcontractors/delegates maintain compliance with requirements of the APL.

ACTIONS:

Please provide a P&P or a completed internal checklist (if no P&P updates are needed) to Regulatory Guidance by **Wednesday May 1, 2024.**

IT002	IT Maintenance Window	Policy Summary: This policy describes Partnership HealthPlan of California (PHC)'s guidelines and procedures for conducting regular scheduled network/systems maintenance on the third Saturday of every month from 12:00 a.m. (Saturday) to 11:59 p.m. (Saturday). This schedule allows for Information Technology (IT) standard maintenance work to be performed. Changes include: • Updated review and revision dates • Updated CEO signature line and date. • Policy Section A Recommendations: • Requesting a schedule change for the IT Network/System maintenance activities to be scheduled for the third Saturday of every month from 12:00 a.m. (Saturday) to 04:00 a.m. (Sunday). Next Review Date: 12/01/2024 Last Review Date: 12/01/2023
IT003	Data Backup	Policy Summary: This policy establishes the Information Systems emergency mode operation plan to enable continuation of critical business processes and protect the Security of Electronic Health Information (ePHI) Changes include: • Updated review and revision dates • Updated CEO signature line and date • Updated Definitions • Updated Policy/Procedure Section A, 1-7 Section B , 1-2 Section C Section D Section E Section G 1c 2 a-f Section H 2-3 Section J Recommendations: • Updated Purpose to removed repetitive verbiage and added weekly and monthly backups to the policy. Next Review Date: 12/01/2024 Last Review Date: 12/01/2023

IT004	IT Application Request	Policy Summary: This policy is for All IT requests for Application Development will be submitted to the IT Department by using the IT WorkFront Application Request Form found in the WorkFront system. Changes include: • Updated review and revision dates. • Updated CEO signature line and date. • No changes to policy or procedure requested. Recommendations: • Next Review Date: 12/01/2024 Last Review Date: 12/01/2023
IT005	IT Steering Committee Charter	Policy Summary: Changes include: • Updated review and revision dates • Updated CEO signature line and date. • No changes to policy or procedure requested. Recommendations: • Next Review Date: 12/01/2024 Last Review Date: 12/01/2023
IT008	Risk Analysis and Management	Policy Summary: This policy establishes the scope, objectives, and procedures of Partnership HealthPlan's (PHC) information security risk management process. Changes include: • Updated review and revision dates • Updated CEO signature line and date. • No changes to policy or procedure requested. Recommendations: • Next Review Date: 12/01/2024 Last Review Date: 12/01/2023

IT010	Sanction Policy	Policy Summary: The purpose of this policy is to establish and apply appropriate sanctions against members of Partnership HealthPlan of California's workforce who fail to comply with Partnership HealthPlan of California's security policies and procedures. Changes include: • Updated to the most recent version of the policy template. • Updated review and revision dates • Updated CEO signature line and date. • No changes to policy or procedure requested. Recommendations: • Next Review Date: 12/01/2024 Last Review Date: 12/01/2023
IT011	Information System Activity Review	Policy Summary: The purpose of this policy to ensure that PHC conducts periodic internal system reviews of system logs or records to minimize security violations to electronic Protected Health Information (ePHI). Changes include: • Updated review and revision dates • Updated CEO signature line and date. • No changes to policy or procedure requested. Recommendations: • Next Review Date: 12/01/2024 Last Review Date: 12/01/2023
IT012	Assigned Security Responsibility	Policy Summary: The purpose of this policy is to ensure PHC conducts periodic internal system reviews of system logs or records to minimize security violations to electronic Protected Health Information (ePHI) and will implement procedures for regular review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Changes include: • Updated review and revision dates • Updated CEO signature line and date. • No changes to policy or procedure requested. Recommendations: Next Review Date: 12/01/2024 Last Review Date: 12/01/2023

IT013	Workforce Security	Policy Summary: This policy is to ensure that all workforce members have appropriate levels of access to electronic Protected Health Information (ePHI) and to prevent those personnel who do not have access to such information from obtaining access to ePHI. Changes include: • Updated review and revision dates • Updated CEO signature line and date. • Updated Policy and Procedure VI Section B 7a-c 8 Recommendations: Next Review Date: 12/01/2024 Last Review Date: 12/01/2023
IT039	Laptop Policy	Policy Summary: The following laptop policy helps achieve this objective by establishing a standard for use that protects ePHI and sensitive company information, while providing enough flexibility to enable employees to complete work in the most efficient and accurate manner. Changes include: • Updated review and revision dates • Updated CEO signature line and dates • Updated Policy and Procedure A, Section 5 Recommendations: • At the request of HR – recommended to add in the event that the laptop is lost or stolen, employee should report the loss immediately to IT Operations, RAC, and your direct report or designee. Next Review Date: 06/01/2024 Last Review Date: 12/01/2023
IT046	274 Provider Directory Data Submission and Issue Resolution Process	Policy Summary: The purpose of the policy is to ensure that Partnership HealthPlan is meeting DHCS requirements for producing the 274 provider directory files for Medi-Cal and DMC ODS programs, and making every effort to convey quality data which accurately represents PHC's provider network. To document the workflow, roles and responsibilities for the 274 provider data file submissions and issue resolution process. Changes include: • Updated review and revision dates • Updated CEO signature line and dates • Updated Policy and Procedure VI, Section A1 a-e, 3a, g1 Recommendations: • EDI requested updates and changes above. Next Review Date: 06/01/2024 Last Review Date: 12/01/2023

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

Policy/Procedure Number: IT002				**Lead Department: IT**	
Policy/Procedure Title: IT Maintenance Window				☐ **External Policy** ☒ **Internal Policy**	
Original Date: 04/04/2014			**Next Review Date:** ~~02/01/2025~~12/01/2023 **Last Review Date:** ~~02/01/2024~~12/01/2024		
Applies to:	☐ **Medi-Cal**		☒ **Employees**		
Reviewing Entities:	☐ **IQI**		☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**		☐ **EXECUTIVE**	☒ **COMPLIANCE**	☒ **DEPARTMENT**
Approving Entities:	☐ **BOARD**		☐ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO**	☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: ~~*Elizabeth Gibboney*~~*Sonja Bjork*				**Approval Date:** ~~06/07/2023~~06/07/2023	

I. RELATED POLICIES:

A. IT049 IT Notification of Unplanned Outages

II. IMPACTED DEPTS:

A. All Departments

III. DEFINITIONS:

A. Maintenance Window is the projected time when a service will be unavailable.

IV. ATTACHMENTS:

A. N/A

V. PURPOSE:

This policy describes Partnership HealthPlan of California (PHC)'s guidelines and procedures for conducting regular scheduled network/systems maintenance on the third Saturday of every month from 12:00 a.m. (Saturday) to 11:59 p.m. (Saturday). This schedule allows for Information Technology (IT) standard maintenance work to be performed.

This policy helps to utilize maintenance windows to:

A. Provide a regularly scheduled planned outage period when routine preventative maintenance can be performed at a time when the business impact is minimal.
B. Improve the security, reliability and performance of the PHCs networking infrastructure and systems
C. Reduce emergency IT outages due to preventative maintenance activities
D. Reduce length of average outage time due to regular maintenance activities
E. Allow staff to better plan their activities that may coincide with scheduled maintenance windows

VI. POLICY / PROCEDURE:

A. IT Network/System maintenance activities will be scheduled on third Saturday of every month from 12:00 a.m. (Saturday) to 04:00 ~~ap~~.m. (~~Saturday~~Sunday).
B. The maintenance window may be adjusted due to any major events requiring IT resources or a longer period to perform maintenance.

Policy/Procedure Number: IT002		Lead Department: IT
Policy/Procedure Title: IT Maintenance Window		☐ **External Policy** ☒ **Internal Policy**
Original Date: 04/04/2014		**Next Review Date:** **02/01/202512/01/2023** **Last Review Date: 02/01/202412/01/2024**
Applies to:	☐ **Medi-Cal**	**Employees**

C. A maintenance window may not always have maintenance activities scheduled for the full window time or there may not be maintenance activities scheduled at all; however, if non-emergency maintenance is required, it will occur during the mentioned scheduled time.
D. Emergency IT issues may arise that could require maintenance activities to occur outside of these windows.
E. Network and system maintenance or outages shall be communicated according to ~~IT Policy's~~ IT049 IT Notification of Unplanned Outages policy

VII. REFERENCES:
A. N/A

VIII. DISTRIBUTION:
A. PowerDMS

IX. DEPARTMENT RESPONSIBLE FOR IMPLEMENTING PROCEDURE: Director, Network Operations

X. REVISION DATES:
A. 10/13/2015
B. 06/21/2017
C. 01/15/2021
D. 12/01/2022
~~D.~~E. 02/01/2024

PREVIOUSLY APPLIED TO:

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

Policy/Procedure Number: IT003			**Lead Department: IT**	
Policy/Procedure Title: Data Backup			☐ **External Policy** ☒ **Internal Policy**	
Original Date: 07/23/2012		**Next Review Date:** ~~12/01/2022~~~~12/01/2023~~12/01/2024 **Last Review Date:** ~~07/05/2022~~~~12/01/2022~~12/01/2023		
Applies to:	☒ **Medi-Cal**	☐ ~~**Healthy Kids**~~ ☒ **Employees**		
Reviewing Entities:	☐ **IQI**	☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**	☐ **EXECUTIVE**	☒~~☐~~ **COMPLIANCE**	☒ **DEPARTMENT**
Approving Entities:	☐ **BOARD**	☐~~☒~~ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO** ☐ **COO**	☐ **CREDENTIALING**	☐~~☒~~ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: ~~*Elizabeth Gibboney*~~*Sonja Bjork*			**Approval Date:** ~~**08/22/2022**~~	

I. RELATED POLICIES:
A. N/A

II. IMPACTED DEPTS:
A. N/A

III. DEFINITIONS:
A. ~~Commvault/Rubrik~~Enterprise Backup – PHC's collective enterprise backup system (currently Commvault/Rubrik)

IV. ATTACHMENTS:
A. N/A

V. PURPOSE:
A. This policy establishes the Information Systems emergency mode operation plan to enable continuation of critical business processes and protect the Security of Electronic Health Information (ePHI) with the intent:

~~*(Note from Leslee: tracked changes shows this entire section was changed but I only updated #5 below)*~~

~~A. To safeguard the information assets of Partnership Health Plan of CA.~~
~~B. To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, power outage, natural disaster or other disruption of critical business operations.~~
~~C. To permit timely restoration of information and business processes, should such events occur.~~
~~D. To manage and secure backup and restoration processes and the media employed in the process.~~
~~E. This policy applies to all servers.~~
~~F. The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.~~
~~G. Backup retention periods are in contrast to retention periods defined by legal or business requirements.~~

Commented [KH1]: *(Note from Leslee: tracked changes shows this entire section was changed but I only updated #5 below)*

Formatted: Font: 10.5 pt

Formatted: List Paragraph, Outline numbered + Level: 2 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Font: Italic, Highlight

Formatted: Font: Italic, Highlight

Formatted: Font: Italic

Formatted: Font color: Yellow

Formatted: Indent: Left: 0.75"

Policy/Procedure Number: IT003		Lead Department: IT
Policy/Procedure Title: Data Backup		☐ **External Policy** ☒ **Internal Policy**
Original Date: 07/23/2012		**Next Review Date: 12/01/202212/01/202312/01/2024** **Last Review Date: 07/05/202212/01/202212/01/2023**
Applies to:	☒ **Medi-Cal**	~~**Healthy Kids**~~ ☒ **Employees**

1. To safeguard the information assets of Partnership Health Plan of CA.
2. To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, power outage, natural disaster or other disruption of critical business operations.
3. To permit timely restoration of information and business processes, should such events occur.
4. To manage and secure backup and restoration processes and the media employed in the process.
5. This policy applies to all servers, including but not limited to file, application, database, Exchange, and virtual servers.
6. The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.
7. Backup retention periods are in contrast to retention periods defined by legal or business requirements.

Formatted: Font: 10.5 pt

VI. POLICY / PROCEDURE:

~~Systems will be backed up according to the schedule below:~~

Systems will be backed up according to the procedure below:

A. ~~Commvault/Rubrik~~ Enterprise Backup (Onsite)

1. All ~~B~~backups are stored on ~~a~~ physical storage (Backup Grid) located in the Server Room at Fairfield headquarters.
2. Daily Backup (Mon-Sat): performed daily with a retention period of (2) two weeks.
   a. Snapshots are taken of file servers exclusively every (4) four hours with a retention period of (7) seven days.
3. Weekly Backup: performed every week on Fridays with a retention period of (4) four weeks.
4. Monthly Backup: performed the last day of the month with a retention period of (1) one year.
5. Yearly Backup: performed the last day of the calendar year with a retention period of (7) seven years.
6. SQL Server/Oracle Log Backup: performed every 60 minutes with a retention period of (7) seven days.
   a. Archived logs from SQL/Oracle hosts will have a retention period of (10) ten days.
7. Snapshots are stored in Rubrik for 30 days. On the 31st day, snapshots are moved offsite.

Formatted: Underline

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Indent at: 1"

~~1.~~

~~2. Monthly Full Archive backup of all servers which includes File, Application, Exchange, Virtual and Database Servers. Monthly Archives are processed the last day of the month and are retained up to 1 year in accordance with business guidelines.~~

~~Daily Full Backup (Mon-Sat): All servers which include File, Application and Database Server are backed up daily and have a retention period on (2) two weeks.~~

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Indent at: 1"

Formatted: No bullets or numbering

Formatted: Underline

B. ~~Commvault/Rubrik~~ Enterprise Backup (Offsite)

1. Backups will be replicated to an offsite ~~Commvault/Rubrik~~ backup server. These backups will match the backup files contained locally and carry the same retention periods as stated in section A above.
2. In certain circumstances based on system compatibility, Commvault and/or Rubrik shall be used for data backup.

Formatted: Indent: Left: 1", No bullets or numbering

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.56" + Indent at: 0.81"

C. All backup data is encrypted in flight using industry-standard HTTPS/TLS (TLS 1.2+) during the

Policy/Procedure Number: IT003		Lead Department: IT
Policy/Procedure Title: Data Backup		☐ **External Policy** ☒ **Internal Policy**
Original Date: 07/23/2012		**Next Review Date: 12/01/202212/01/202312/01/2024** **Last Review Date: 07/05/202212/01/202212/01/2023**
Applies to:	☒ **Medi-Cal**	~~**Healthy Kids**~~ ☒ **Employees**

transfer and at rest using AES-256 encryption.

~~2.~~D. New servers introduced to PHC's development and/or production environment will have backup requirements assessed prior to deployment. The server owner will provide IT Operations of backup requirements and justification. Upon approval, the server(s) will be added to the enterprise backup system with backup jobs being validated per policy.

~~C.~~E. A log of ~~Commvault/Rubrik servers~~the back-up schedule will be maintained by the enterprise backup system and reviewed by PHC's HIPAA Security Officer and/or designee.

~~D.~~F. Media will be retired and disposed of as described below:

1. Prior to retirement and disposal, IT will ensure that:

   a. The media no longer contains active backup images
   b. The media's current or former contents cannot be read or recovered by an unauthorized party.
   c. With all backup media, IT will ensure the physical destruction of media prior to disposal.

~~E.~~ Backups will be verified periodically: ~~(Onsite Backup)~~

G.

1. Onsite Backups
   ~~1.~~a. On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:
      ~~2.~~i. To check for and correct errors.
      ~~3.~~ii. To monitor the duration of the backup job.
      ~~4.~~iii. To optimize backup performance where possible.
   ~~5.~~b. IT will identify problems and take corrective action to reduce any risks associated with failed backups.
   ~~6.~~c. Random ~~test~~ restores will be~~are~~~~will be~~ performed~~done~~ once a week in order to verify that backups have been successful and to ensure data reliability and integrity.
   ~~7.~~d. IT will maintain records demonstrating the review of logs and test restores to demonstrate compliance with this policy for auditing purposes.
   e. Ensure replication of data from onsite to offsite backup grid occurs.
2. Offsite Backups
   a. Random restores will be performed quarterly in order to ensure data reliability and integrity.
   b. IT will identify problems and take corrective action to reduce any risks associated with failed restores.
   c. IT will maintain records demonstrating the review of logs and test restores to demonstrate compliance with this policy for auditing purposes.
   d. Quarterly reports will be generated and will include the following:
      i. Results of the test restores
      ii. Root cause analysis of any failures
      iii. Backup capacity at the time of the restore
      iv. Validation of secure storage
   e. Annual reports will be generated at the end of each calendar year and will include the following:
      i. Annual failure report
      ii. Backup capacity and future capacity forecast

Formatted: Indent: Left: 0.81", No bullets or numbering

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.56" + Indent at: 0.81"

Formatted: Font: 10.5 pt

Formatted: CM8, Justified, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.56" + Indent at: 0.81"

Formatted

Formatted

Formatted

Policy/Procedure Number: IT003		Lead Department: IT
Policy/Procedure Title: Data Backup		☐ **External Policy** ☒ **Internal Policy**
Original Date: 07/23/2012	**Next Review Date: 12/01/202212/01/202312/01/2024** **Last Review Date: 07/05/202212/01/202212/01/2023**	
Applies to: ☒ **Medi-Cal**	~~**Healthy Kids**~~ ☒ **Employees**	

f. Quarterly and annual reports will be furnished to the HIPAA Security Officer and other executive leadership as deemed appropriate for review and acknowledgment

~~8.~~

~~F.~~H. Data Recovery

1. In the event of a catastrophic system failure, off-site backed up data will be restored as per the Disaster Recovery Plan.
2. In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within durations assigned by the company's business impact analysis (BIA) guidelines.
~~2.~~3. All transaction-based systems are database driven, and are to be backed up at the database level inclusive of all data and transactions logs. These logs ~~can~~will be utilized for transaction recovery as needed.

~~G.~~I. Restoration Requests

1. In the event of accidental deletion or corruption of information, requests for restoration of information will be made to the IT Service Desk. An assigned System administrator will perform all recovery or restoration process.

~~H.~~J. Responsibilities:

1. Backups and Data~~e~~ Recovery: IT Network Storage Engineer ~~Systems Administrators~~
2. Verification: System, Application, and Data~~s~~ ~~Administrator~~Owners
3. ~~Authorized Transport: Systems Administrators and Managers~~

VII. REFERENCES:

A. 45 CFR 164.308 7(ii)(a) Data Backup Plan - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information

VIII. DISTRIBUTION:

A. PowerDMS

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE: Director IT Operations

X. REVISION DATES:

A. 10/19/2014
B. 06/22/2017
C. 01/15/2021
D. 07/05/2022
~~D.~~E. 12/01/2023~~2~~

PREVIOUSLY APPLIED TO:

A. N/A

Formatted

Formatted: Font: 12 pt

Formatted: Normal, Left, Indent: Left: 1", No bullets or numbering

Formatted: Font: 10.5 pt

Formatted: List Paragraph, Left

Formatted: Font: 10.5 pt

Policy/Procedure Number: IT003			**Lead Department: IT**
Policy/Procedure Title: Data Backup			☐ **External Policy** ☒ **Internal Policy**
Original Date: 07/23/2012		**Next Review Date: 12/01/202212/01/202312/01/2024** **Last Review Date: 07/05/202212/01/202212/01/2023**	
Applies to:	☒ **Medi-Cal**	~~**Healthy Kids**~~ ☒ **Employees**	

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

Policy/Procedure Number: IT004				**Lead Department: IT**	
Policy/Procedure Title: IT Application Request				☐ **External Policy** ☒ **Internal Policy**	
Original Date: 09/16/2013			**Next Review Date:** ~~12/01/2023~~12/01/2024 **Last Review Date:** ~~12/01/2022~~12/01/2023		
Applies to:	☐ **Medi-Cal**		☐ **Healthy Kids**	☒ **Employees**	
Reviewing Entities:	☐ **IQI**		☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**		☐ **EXECUTIVE**	☒ **COMPLIANCE**	☒ **DEPARTMENT**
Approving Entities:	☐ **BOARD**		☐ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO**	☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: ~~*Elizabeth Gibboney*~~*Sonja Bjork*				**Approval Date:** ~~02/27/2023~~02/27/2023	

I. RELATED POLICIES:

A. N/A

II. IMPACTED DEPTS:

A. N/A

III. DEFINITIONS:

A. **Project:** Any New Application Development that is estimated to be more than 40 hours.

IV. ATTACHMENTS:

A. N/A

PURPOSE: All IT requests for Application Development will be submitted to the IT Department by using the IT WorkFront Application Request Form found in the WorkFront system.

V. POLICY / PROCEDURE:

A. Users will submit an online IT Application Request form found at https://phc.my.workfront.com/requests?activeTab=tab-new-helpRequest&projectID=56b4dc77002aac14f14d4e95d18b8627&path. Once submitted, the request will be assigned a Submitter ID in which the requestor can use to follow status or provide updates to the request.

B. IT management will review each submitted request and determine if the request is a project, maintenance or an enhancement.
   1. For each approved maintenance or enhancement request, IT Management will assign a support team or person to work with the requesting stakeholder, and perform and complete the work.
   2. For each rejected maintenance or enhancement request, the relevant stakeholder will be notified of the decision, suggesting a workaround, if possible. In both cases, the IT application request record will be updated accordingly.
   3. For each project, IT Management will either approve or send to IT Steering Committee for approval.

C. If approved, IT will assign an IT team to the request. If a larger project, a Project Manager will be assigned.

Policy/Procedure Number: IT004		Lead Department: IT	
Policy/Procedure Title: IT Application Request		☐ **External Policy** ☒ **Internal Policy**	
Original Date: 09/16/2013		**Next Review Date: 12/01/202312/01/2024** **Last Review Date: 12/01/202212/01/2023**	
Applies to:	☐ **Medi-Cal**	☐ **Healthy Kids**	☒ **Employees**

VI. REFERENCES:
A. N/A

VII. DISTRIBUTION:
A. PowerDMS

VIII. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE: All employees

IX. REVISION DATES:
10/13/2013
11/29/2021
12/01/2022

PREVIOUSLY APPLIED TO:

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

<table>
<tr><td colspan="3">Policy/Procedure Number: IT005</td><td colspan="3">Lead Department: IT</td></tr>
<tr><td colspan="3">Policy/Procedure Title: IT Steering Committee Charter</td><td colspan="3">☐ External Policy
☒ Internal Policy</td></tr>
<tr><td colspan="2">Original Date: 09/16/2013</td><td colspan="4">Next Review Date: ~~12/01/2023~~12/01/2024
Last Review Date: ~~12/01/2022~~12/01/2023</td></tr>
<tr><td>Applies to:</td><td colspan="2">☒ Medi-Cal</td><td colspan="3">~~☐ Healthy Kids~~
☒ Employees</td></tr>
<tr><td rowspan="2">Reviewing Entities:</td><td colspan="2">☐ IQI</td><td>☐ P & T</td><td>☐ QUAC</td><td></td></tr>
<tr><td colspan="2">☐ OPERATIONS</td><td>☐ EXECUTIVE</td><td>☒ COMPLIANCE</td><td>☒ DEPARTMENT</td></tr>
<tr><td rowspan="2">Approving Entities:</td><td colspan="2">☐ BOARD</td><td>☐ COMPLIANCE</td><td>☐ FINANCE</td><td>☐ PAC</td></tr>
<tr><td>☒ CEO</td><td>☐ COO</td><td>☐ CREDENTIALING</td><td colspan="2">☐ DEPT. DIRECTOR/OFFICER</td></tr>
<tr><td colspan="3">Approval Signature: ~~Elizabeth Gibboney~~Sonja Bjork</td><td colspan="3">Approval Date: ~~02/22/2023~~02/22/2023</td></tr>
</table>

I. RELATED POLICIES:
A. N/A

II. IMPACTED DEPTS:
A. N/A

III. DEFINITIONS:
A. N/A

IV. ATTACHMENTS:
A. N/A

V. PURPOSE:

VI. POLICY / PROCEDURE:

The IT Steering Committee is responsible for conducting final review and prioritization on all technology projects, ensuring compliance with HIPAA and state requirements, and addressing project related issues. All members have a stake in IT's relationship to PHC business and are expected to attend the monthly meetings. In the event that a Steering Committee member is unable to attend, a representative should be sent in their place that has the authority to make decisions on that member's behalf.

The IT Steering Committee will use submitted IT Application Requests to review new application development projects. This form and the request dashboard can be found at: https://phc.my.workfront.com/requests?activeTab=tab-new-helpRequest&projectID=56b4dc77002aac14f14d4e95d18b8627&path

A. The IT Steering Committee will meet monthly to perform the following as needed: review and approve or reject projects and project charters, plans, milestones, status reports and dashboards; prioritize projects; review IT strategic plans and service level agreements (SLAs); address technology and project related issues; and assist in defining and monitoring

the IT department's role in meeting company objectives.

VII. REFERENCES:
A. N/A

VIII. DISTRIBUTION:
A. PowerDMS

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE: Executive Team, and IT Steering Committee Members

X. REVISION DATES:
10/13/2014
03/01/2022
12/01/2022

PREVIOUSLY APPLIED TO:
N/A

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

<table>
<tr><td colspan="3">Policy/Procedure Number: IT008</td><td colspan="3">Lead Department: IT</td></tr>
<tr><td colspan="3">Policy/Procedure Title: Risk Analysis and Management</td><td colspan="3">☐ External Policy
☒ Internal Policy</td></tr>
<tr><td colspan="2">Original Date: 05/21/2014</td><td colspan="4">Next Review Date: ~~12/01/2022~~12/01/2024
Last Review Date: ~~07/05/2022~~12/01/2023</td></tr>
<tr><td>Applies to:</td><td colspan="2">☐ Medi-Cal</td><td colspan="3">☒ Employees</td></tr>
<tr><td rowspan="2">Reviewing Entities:</td><td colspan="2">☐ IQI</td><td>☐ P & T</td><td>☐ QUAC</td><td></td></tr>
<tr><td colspan="2">☐ OPERATIONS</td><td>☐ EXECUTIVE</td><td>☒ COMPLIANCE</td><td>☐ DEPARTMENT</td></tr>
<tr><td rowspan="2">Approving Entities:</td><td colspan="2">☐ BOARD</td><td>☐~~☒~~ COMPLIANCE</td><td>☐ FINANCE</td><td>☐ PAC</td></tr>
<tr><td>☒ CEO</td><td>☐ COO</td><td>☐ CREDENTIALING</td><td colspan="2">☐~~☒~~ DEPT. DIRECTOR/OFFICER</td></tr>
<tr><td colspan="3">Approval Signature: ~~Elizabeth Gibboney~~Sonja Bjork</td><td colspan="3">Approval Date: ~~08/22/2022~~08/22/2022</td></tr>
</table>

I. RELATED POLICIES:

A. CMP24 Physical and Administrative Safeguards
B. CMP28 Training Program Requirements
C. IT010 Sanction Policy

II. IMPACTED DEPTS:

A. N/A

III. DEFINITIONS:

A. Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.
B. Risk: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information, and other system assets.
C. Risk Analysis: the process:
    1. Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;
    2. Prioritizes risks;
    3. Results in recommended possible actions/controls that could reduce or offset the determined risk.
D. Risk Management: is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.
E. Threat: the potential for a particular threat-source to successfully exercise a particular vulnerability.
    1. Threats are commonly categorized as:
        a. Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
        b. Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
        c. Natural – fires, floods, electrical storms, tornados, etc.
        d. Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
        e. Other – explosions, medical emergencies, misuse or resources, etc.

Policy/Procedure Number: IT008		Lead Department: IT
Policy/Procedure Title: Risk Analysis and Management		☐ **External Policy** ☒ **Internal Policy**
Original Date: 05/21/2014		**Next Review Date: 12/01/2024~~3~~** **Last Review Date: ~~07/05/2022~~12/01/2023**
Applies to:	☐ **Medi-Cal**	~~Error! No text of specified style in document. **Healthy Kids**~~ ☒ **Employees**

F. Threat Source – Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the organization's ability to protect ePHI.

G. Threat Action – The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

H. Vulnerability: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system. Resulting in a security breach or violation of policy.

IV. ATTACHMENTS:

A. Risk Management Plan Template

V. PURPOSE:

This policy establishes the scope, objectives, and procedures of Partnership HealthPlan's (PHC) information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission by taking effective steps to minimize or eliminate any potential risks and vulnerabilities to the electronic protected health information (ePHI) created, received, processed, transmitted or held by a business associate.

VI. POLICY / PROCEDURE:

A. Policy

Scope: The scope of the information security risk mitigation process covers the administrative, physical, and technical processes that govern ePHI that is received, created, maintained or transmitted.

1. PHC shall conduct HIPAA Risk Analysis at least annually to comply with the Health Insurance ~~Probability~~ Portability and Accountability~~tably~~ Act (HIPAA) Security Rule, as amended to ensure thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its ePHI (and other confidential and proprietary electronic information) and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the organization's information security program.
2. Risk mitigation is recognized as an important component of PHC's compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8).
   a. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of PHC's HIPAA Information Security Officer, or his/her designee.
   b. The HIPAA Security Officer shall advise the Chief Executive Officer (CEO) or designee on risk management strategies and provide periodic reports on program progress. The HIPAA Security Officer may advise the PHC Board of Commissioners (Board) whenever there is a significant change in people, processes or technologies related to ePHI that could potentially affect risk.
   c. The annual risk analysis shall be performed externally by a qualified business associate.
   d. PHC, at the direction of the HIPAA Security Officer or securities designee shall perform periodic technical and non-technical assessments of the security rule requirements as well as in response to

environmental or operational changes affecting the security of ePHI.

3. Through risk mitigation, PHC shall ensure the implementation and maintenance of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
   a. Ensure the confidentiality, integrity, and availability of all ePHI the organization creates, receives, maintains, and/or transmits.
   b. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
   c. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required.
   d. Ensure compliance by workforce.
4. All PHC workforce members shall be expected to fully cooperate with all persons charged with doing risk mitigation work. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation according to PHC IT Sanction policy, IT010. All applicable workforce members shall be trained regarding their appropriate responsibilities and duties to reduce the risk of security incidents. Such training shall be incorporated into annual security & awareness training materials in accordance with PHC policies CMP28 and CMP24.
5. National Institute of Standards and Technology (NIST), specifically SP800- 30 will be utilized as framework for conducting Risk Analysis. The risk analysis shall demonstrate, at a minimum, the following information:
   a. The level of risk associated with each potential vulnerability exploitation;
   b. Steps to be taken to reduce the risk of vulnerability exploitation;
   c. Processes for maintaining no more than the acceptable level of risk.

B. Procedures:
   1. Risk Analysis procedures must involve the following steps:
      a. Obtain information regarding ePHI assets identified per the requirement in HIPAA Security Management Process standard, including the criticality and sensitivity of each asset. (See section IV, References.)
      b. Identify the vulnerabilities that these assets may have or be associated with in their day-to-day operations. Consider technical, administrative/process, human, and physical vulnerabilities. Include vulnerabilities that could impact the confidentiality, integrity and availability of data.
      c. Identify the threats that could exploit the vulnerabilities identified. Consider human (intentional and unintentional) and environmental (e.g., weather, air quality) threats. Include threats that could impact the confidentiality, integrity and availability of data.
      d. Evaluate the controls and costs of safeguards (technical and administrative). Incorporate safeguards that produce an expected annual cost savings based on the annual loss expectancy, or are otherwise necessary to meet the requirements of the HIPAA Security Rule or other mandates. Consider the reasonableness and appropriateness of security controls selected, considering factors specific to the organization (e.g., size, environment, operating changes, and configuration).
      e. Estimate the likelihood that a threat would successfully exploit each of the identified vulnerabilities, given the current controls in place to guard against such exploits.
      f. Determine the impact to the organization were the threat able to exploit the vulnerability, given the current control environment. Impact should be evaluated based on protecting the confidentiality, integrity, and availability of ePHI.

2. Risk Management: Risk management involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk analysis and assessment process to ensure the confidentiality, integrity and availability of ePHI.
   a. The HIPAA Security Officer will document risks and develop Risk Management strategy for all critical and high risks, with some actionable medium risks as appropriate. Other mediums and all low risks will be accepted unless otherwise deemed as needing Risk Treatment or Risk Management efforts beyond analysis.
3. Risk Management Schedule: The Risk Management process will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of PHC's information security program:
   a. At the direction of IT, Business Line Managers, shall be responsive to and participate in internal audits that are performed at least once annually on all computing systems and/or business processes under their units' control that involve non-public information, following guidance from the HIPAA Security Officer on assessment method, format, content, and frequency.
   b. Business Line Managers shall submit the audit results and associated remediation plans to the HIPAA Security Officer for review. Remediation plans shall include specific actions with prioritization of risk, as well as an account of residual risks.
   c. Remediation plans should be developed using document template referenced m Attachments section above.
   d. The HIPAA Security Officer may call for a full or partial risk analysis in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect PHC's information systems.
   e. Risk Management Summary will be documented and reviewed with Compliance Committee and IT Steering Committee
4. Process Documentation: PHC shall maintain documentation of all risk analysis, risk management and risk mitigation efforts for a minimum of 6 (six) years.

VII. REFERENCES:

A. Regulatory Authority:
   45 CFR § 164.308(a)(1)(ii)(A)
   45 CFR § 164.308(a)(1)(ii)(B)

B. External:
   1. Health and Human Services - Office of Civil Rights, "Final Guidance on Risk Analysis", http://www.hhs.govIocr/privacy/hipaa/administrntive/securityrule/rafinalguidancepdf.pdf
   2. National Institute of Standards and Technology (NIST) Special Publication 800-30 Revision 1, " Guide for Conducting Risk Assessment" http://csrc.nist.gov/publications/nistpubs/800-30-rev_l/sp800_30_r I .pdf
   3. National Institute of Standards and Technology (NIST) Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations" http ://nvlpubs.nist. gov/nistpubs/SpecialPublications/NIS T. SP.800-53r4.pdf
   4. Omnibus Final Rule: http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=al 031c979l 26e6440b522063b7bba578&rgn=div5&view=text&node=45:1.0.1.3. 78&idno=45%20
   5. "HIPAA Security Final Rule" http://www.ecfr.gov/cgi-bin/text-

Policy/Procedure Number: IT008		Lead Department: IT
Policy/Procedure Title: Risk Analysis and Management		☐ **External Policy** ☒ **Internal Policy**
Original Date: 05/21/2014		**Next Review Date: 12/01/2024~~3~~** **Last Review Date: ~~07/05/2022~~12/01/2023**
Applies to:	☐ **Medi-Cal**	~~Error! No text of specified style in document. **Healthy Kids**~~ ☒ **Employees**

idx?c=ecfr&SID=al
031c979126e6440b522063b7bba578&rgn=div5&view=text&node=45: 1.0.l .3.78&idno=45%20

VIII. DISTRIBUTION:
A. PowerDMS

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE: HIPAA Security Officer, Director, Network Operations

X. REVISION DATES: 05/16/2016, 07/05/2022

PREVIOUSLY APPLIED TO: N/A

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY / PROCEDURE

Policy/Procedure Number: IT010				**Lead Department: IT**	
Policy/Procedure Title: Sanction Policy				☐ **External Policy** ☒ **Internal Policy**	
Original Date: 04/01/2014			**Next Review Date:** ~~12/01/2023~~12/02/2024 **Last Review Date:** ~~07/05/2022~~12/01/2023		
Applies to:	☐ **Medi-Cal**		☒ **Employees**		
Reviewing Entities:	☐ **IQI**		☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**		☐ **EXECUTIVE**	☒ **COMPLIANCE**	☒ **DEPARTMENT**
Approving Entities:	☐ **BOARD**		☐ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO**	☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: ~~*Elizabeth Gibboney*~~*Sonja Bjork*				**Approval Date:** ~~08/22/2022~~	

Formatted: Font color: Red, Strikethrough

I. RELATED POLICIES:

II. IMPACTED DEPTS:

III. DEFINITIONS:

IV. ATTACHMENTS: N/A

V. PURPOSE:

Partnership HealthPlan of California is committed to conducting business in compliance with all applicable laws, regulations and Partnership HealthPlan of California policies related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and, specifically, Subpart C Security Standards for the protection of electronic Protected Health Information (ePHI) of PART 164 Security and Privacy. Part of that commitment is to ensure that Partnership HealthPlan of California applies appropriate penalties against workforce members who fail to comply with security policies and procedures related to electronic Protected Health Information (ePHI).

As required in 45 C.F.R. § 164.308(1)(ii)(C), Sanction Policy, the purpose of this policy is to establish and apply appropriate sanctions against members of Partnership HealthPlan of California's workforce who fail to comply with Partnership HealthPlan of California's security policies and procedures. This policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to sanctioning for violating Partnership HealthPlan of California's policies and procedures.

VI. POLICY / PROCEDURE:

A. Policy

1. Partnership HealthPlan of California will apply appropriate sanctions against members of its workforce and business associates who fail to comply with the Partnership HealthPlan of California policies and procedures or resort to system misuse, abuse or fraudulent activity.
2. The type of sanction applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors.
3. Sanctions may include, but will not be limited to:
   a. Verbal counseling
   b. Written counseling
   c. Conducting additional conferences
   d. Removal of system privileges

Policy/Procedure Number: IT010		Lead Department: IT
Policy/Procedure Title: Sanction Policy		☐ **External Policy** ☒ **Internal Policy**
Original Date: 04/01/2014		**Next Review Date:** ~~12/01/2023~~12/01/2024 **Last Review Date: 07/05/202212/01/2023**
Applies to:	☐ **Medi-Cal**	~~Error! No text of specified style in document.~~ **~~Healthy Kids~~** ☒ **Employees**

e. Suspension or termination of employment
f. Ad hoc training opportunities (in addition to New Hire and Annual)

4. Workforce members, agents, and other contractors should be aware that violations of a severe nature may result in notification to law enforcement officers as well as regulatory, accreditation, and/or licensure organizations.
5. The policy and procedures contained herein do not apply specifically when members of Partnership HealthPlan of California's workforce exercise their right to:
   a. file a complaint with Department of Health and Human Services (DHHS);
   b. testify, assist, or participate in an investigation, compliance review, proceeding, or hearing under Part C of Title XI;
   c. oppose any act made unlawful by the HIPAA Security rule; provided the individual or person has a good faith belief that the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of electronic protected health information in violation of the HIPAA Security rule;
   d. disclose electronic protected health information as a whistleblower and the disclosure is to a health oversight agency; public health authority; or an attorney retained by the individual for purposes of determining the individual's legal options with regard to the whistleblower activity; or
   e. an employee who is a victim of a crime and discloses protected health information to a law enforcement officer, provided that the protected health information is about a suspected perpetrator of the criminal act.
6. The HIPAA Security Officer will work with HR to determine the severity of necessary sanctions.
7. All sanctioning of workforce members will be documented and retained for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.
8. Personnel are hereby advised that in addition to the sanctions outlined in this document, civil and/or criminal penalties may apply.

B. Procedure
1. The HIPAA Security Officer will investigate any allegations of wrongful actions and determine and apply the appropriate sanction(s) in conjunction with Human Resources.
2. PHC has established the following sanctions apply for failure to comply with Partnership HealthPlan of California policies or procedures or with the requirements of HIPAA regulations:
   a. first offense of noncompliance = verbal counseling
   b. second offense of noncompliance = (formal) written counseling
   c. third offense of noncompliance = suspension without pay or termination PHC may elect to conduct additional conferences with the employee.
3. All investigations and sanctioning actions will be documented by HIPAA Security Officer and securely stored.
4. All sanctioning of workforce members will be documented and retained for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.
5. The HIPAA Security Officer will notify law enforcement, regulatory, accreditation and/or licensure agencies of wrongful actions as appropriate.
6. The HIPAA Security Officer will ensure any necessary changes to personnel clearance and/or access lists are immediately made

Policy/Procedure Number: IT010		Lead Department: IT
Policy/Procedure Title: Sanction Policy		☐ **External Policy** ☒ **Internal Policy**
Original Date: 04/01/2014		**Next Review Date:** ~~12/01/2023~~12/01/2024 **Last Review Date: 07/05/202212/01/2023**
Applies to:	☐ **Medi-Cal**	~~Error! No text of specified style in document.~~ ~~**Healthy Kids**~~ ☒ **Employees**

VII. REFERENCES:

A. Regulatory:

1. 45 C.F.R. § 164.308 Administrative safeguards.
   (a) A covered entity or business associate must, in accordance with § 164.306: (l)(ii) Implementation specifications:
   (C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

B. Internal

1. IT-012 Assigned Security Responsibility
2. CMP-24 HIPAA Privacy Enforcement
3. HR 405 Performance Management

C. External

1. National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1, "A Resource Guide for Implementing The HIPAA Security Rule" http://csrc.nist.gov/publications/PubsSPs.html
2. National Institute of Standards and Technology (NIST) Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems" http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

VIII. DISTRIBUTION:

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE:

X. REVISION DATES:

A. 12/01/2021
B. 07/05/2022

PREVIOUSLY APPLIED TO:

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

Policy/Procedure Number: IT011				**Lead Department: IT**	
Policy/Procedure Title: Information System Activity Review				☐ **External Policy** ☒ **Internal Policy**	
Original Date: 05/14/2014			**Next Review Date:** ~~12/01/2023~~12/01/2024 **Last Review Date:** ~~07/05/2022~~12/01/2023		
Applies to:	☐ **Medi-Cal**		☒ **Employees**		
Reviewing Entities:	☐ **IQI**		☐ **P & T**	☐ **IT STEERING COMMITTEE**	
	☐ **OPERATIONS**		☐ **EXECUTIVE**	☒ **COMPLIANCE**	☒ **DEPARTMENT**
Approving Entities:	☐ **BOARD**		☐ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO**	☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: ~~*Elizabeth Gibboney*~~*Sonja Bjork*				**Approval Date:** ~~08/22/2022~~08/22/2022	

I. RELATED POLICIES:

A. IT012 - Assigned Security Responsibility
B. IT023 - Password Management
C. IT024 - Security Incident Response
D. IT024 - Response and Reporting
E. IT039 - Audit Controls
F. ITDP08 – Credentialing System User Activity Review

II. IMPACTED DEPTS:

A. N/A

III. DEFINITIONS:

A. Security Review - a collaborative process used to identify security-related issues, determine the level of risk associated with those issues, and make informed decisions about the risk mitigation or acceptance.

IV. ATTACHMENTS:

A. N/A

V. PURPOSE:

Partnership HealthPlan of California (PHC) is committed to conducting business in compliance with all applicable laws, regulations and PHC policies related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and, specifically, Subpart C Security Standards for the protection of electronic Protected Health Information (ePHI) of PART 164 – Security and Privacy.

Part of that commitment is to ensure that PHC conducts periodic internal system reviews of system logs or records to minimize security violations to electronic Protected Health Information (ePHI). As such, PHC will continually assess potential risks and vulnerabilities to protected health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with 45 C.F.R. § 164.308. Additionally, as specifically required by 45 C.F.R. § 164.308(1)(ii)(D), Information Systems Review Activity, PHC will implement procedures for regular review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Policy/Procedure Number:		**Lead Department: IT**
Policy/Procedure Title: Information System Activity Review		☐ **External Policy** ☒ **Internal Policy**
Original Date: 05/14/2014		**Next Review Date: 12/01/202312/01/2024** **Last Review Date: 07/05/202212/01/2023**
Applies to:	☐ **Medi-Cal**	~~Error! No text of specified style in document.~~ **~~Healthy Kids~~** ☒ **Employees**

VI. POLICY / PROCEDURE:

A. Policy

1. PHC shall establish procedures for audits and reviews of Information Systems that process or store ePHI to protect against unauthorized Access or use of such ePHI.
2. PHC shall determine reasonable and appropriate audit controls for Information Systems that process or store ePHI, based on its Risk Analysis and organizational factors, such as current technical infrastructure, Hardware, and software Security capabilities.
3. PHC shall perform system Security reviews for Information Systems that process or store ePHI. This review shall be performed in accordance with regulatory, statutory, and contractual guidance, when a significant change to a system or application, or when a system event occurs to trigger a need for a revision.
4. PHC shall ensure that Information Systems that process or store ePHI have established routine procedures to review system Access logs for unauthorized Access.
5. PHC shall ensure that Information Systems that process or store ePHI have a documented change control procedure that protects the Confidentiality, Integrity, and Availability or ePHI.
6. If PHC and its Business Associate become aware of unauthorized Access or use of ePHI, they shall adhere to the policies and procedures set forth in PHC Policy CMP 18: Reporting privacy Incidents and Breach Notifications.
7. PHC and its Business Associates shall apply appropriate Sanctions against its Business Associates and/or Users where there has been a violation of compliance with HIPAA, as amended, and the regulations promulgated thereunder, and/or PHC security policies up to, and including termination of contracts or employment, as applicable and in accordance with PHC Policy IT010: Sanctions.
8. Business Associates shall have policies and procedures as required by the HIPAA Security Rule and that are consistent with their obligations under PHC Business Associate Agreements.
9. PHC will conduct an internal review of its system activity records on a regular, ongoing basis as deemed necessary based on results of the Security Risk Analysis (Refer to Policy IT008. Risk Analysis and Management) or specific business or operational needs.

B. Procedure

1. The HIPAA Security Officer is responsible for managing or directing the conduct of regular reviews of PHC's information systems' activities.
2. PHC shall ensure that Information Security Systems that process or store ePHI have, a minimum, an annual system Security review, which may be a component of the annual risk analysis.
   a. PHC shall include administrative and technical vulnerability scanning tools in their annual system security review.
3. Necessary safeguards to protect the confidentiality, availability and integrity of audit trails and information system activity review reports must be implemented. Such safeguards may be provided by the information system components (e.g., password-protected access to audit logs, file integrity checkers), as well as by organization-defined processes (e.g., regularly backed up audit logs, which are stored in fire-resistant, offsite, locked containers).
4. PHC shall regularly review records of Information Systems activity such as; audit logs, access reports, and Security Incident tracking reports. Review shall include but not be limited to:
   a. Log all system administrator or developer a~~A~~ccess ~~and~~ changes if the system is processing or storing e~~E~~PHI;

b. Log successes and failures of User Authentication at all levels.;
c. Specific checks should include: unsuccessful login or access attempts, log-in events outside of normal business hours, excessive log-ins by a user that may look suspicious, or users logged in for an abnormally long duration. As such, require the workforce member to reset their domain password after a defined interval or specified number of unsuccessful logon attempts, in accordance with ~~PHC~~ IT Policy IT023 Password Management.

5. The audit logs must be retained for a minimum period of 6 years. Procedure for disposal of audit logs after the minimum retention period must be formally documented and implemented, including responsibilities related to disposal.
6. There are system controls in place to ensure the integrity and/or correctness of the information processed, transmitted and/or stored by the information systems, which must identified, documented and implemented.
7. A report is generated that details the review findings. The report should include the system reviewed, date and time of performance, component information (e.g., host id, IP address, component type, etc.), and significant findings describing events requiring additional action (e.g., further investigation, sanctioning, training program adjustments, and/or modifications to safeguards).

C. Conduct

1. For each component identified above, the audit logs are examined for security-significant events with respect to PHC's security policy. On an on-going basis, systems are monitored, via multiple mechanisms, for the following reasons, but not limited to, viruses, malicious content, ensure password integrity and inappropriate log-on attempts. One such mechanism utilized is 24/7 by 365 monitoring.
2. The applicable human-generated records of the receipt, initial handling, access, removal, and disposal of system hardware, software, and media containing patient data for consistency with PHC's security policy are reviewed.
3. Review findings and recommendations are presented to the appropriate management of PHC.
4. An audit calendar will be maintained for the review of system activity.

D. Follow-up

1. Findings and recommendations will be incorporated into PHC's security training program and other interventions as appropriate.
2. Adjustments to the administrative, physical and technical safeguards will be made as necessary based on the review findings. As appropriate, PHC shall employ a change review process wherein the individual who identified the risk is not the individual approving necessary system changes and shall seek approval from respective IT leadership.
3. Review findings Information System activity review shall be completed to meet its Risk Management strategy and account for the capabilities of all Information Systems that process or store ePHI.

E. The policies and procedures established herein, including all derivative documents regarding information system activity reviews will be documented and maintained in a current manner.

VII. REFERENCES:

A. Regulatory

Policy/Procedure Number:		Lead Department: IT
Policy/Procedure Title: Information System Activity Review		☐ **External Policy** ☒ **Internal Policy**
Original Date: 05/14/2014		**Next Review Date: 12/01/202312/01/2024** **Last Review Date: 07/05/202212/01/2023**
Applies to:	☐ **Medi-Cal**	~~Error! No text of specified style in document.~~ **~~Healthy Kids~~** ☒ **Employees**

45 C.F.R. § 164.308 Administrative Safeguards

(a) A covered entity or business associate must, in accordance with § 164.306:

(1) (ii) *Implementation specifications:*

(D) *Information system activity review* (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

B. Internal

C. External

1. National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1, "A Resource Guide for Implementing The HIPAA Security Rule" (http://csrc.nist.gov/publications/PubsSPs.html)
2. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 3 Final, "Recommended controls for Federal Information Systems and Organizations " (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)
3. ational Institute of Standards and Technology (NIST) Special Publication " Guide to Computer Security Log Management " (http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf)
4. National Institute of Standards and Technology (NIST) Special Publication 800-122 Revision 3 Final, " Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf)
5. ational Institute of Standards and Technology (NIST) Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems" (http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf)
6. National Institute of Standards and Technology (NIST) Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices (http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

VIII. DISTRIBUTION:
A. PowerDMS

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE: HIPPA Security Officer

X. REVISION DATES:

A. 11/19/2019
B. 06/24/2022
C. 07/05/2022

XI. PREVIOUSLY APPLIED TO:
A. N/A

Policy/Procedure Number:			**Lead Department: IT**
Policy/Procedure Title: Information System Activity Review			☐ **External Policy** ☒ **Internal Policy**
Original Date: 05/14/2014		**Next Review Date: 12/01/202312/01/2024** **Last Review Date: 07/05/202212/01/2023**	
Applies to:	☐ **Medi-Cal**	~~Error! No text of specified style in document.~~ **~~Healthy Kids~~** ☒ **Employees**	

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

Policy/Procedure Number: IT012				**Lead Department: IT**	
Policy/Procedure Title: Assigned Security Responsibility				☐ **External Policy** ☒ **Internal Policy**	
Original Date: 05/14/2014			**Next Review Date:** ~~12/01/2023~~12/01/2024 **Last Review Date:** ~~07/05/2022~~12/01/2023		
Applies to:	☒ **Medi-Cal**		☒ **Employees**		
Reviewing Entities:	☐ **IQI**		☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**		☐ **EXECUTIVE**	☒ **COMPLIANCE**	☐ **DEPARTMENT**
Approving Entities:	☐ **BOARD**		☐ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO**	☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: ~~*Elizabeth Gibboney*~~*Sonja Bjork*				**Approval Date:** ~~08/22/2022~~08/22/2022	

I. RELATED POLICIES:

A. CMP 23-External PHI Release Control
B. IT008 Risk Analysis and Management
C. IT010 Sanctions

II. IMPACTED DEPTS:

A. N/A

III. DEFINITIONS:

A. Business Associate: As defined in 45 C.F.R. § 160.103, a business associate is a person or entity that performs certain functions that involve the use or disclosure of protected health information (PHI) on behalf of, or provides services, to a covered entity.
B. Administrative Safeguards: Formal mechanisms for risk analysis and management, information access controls, and appropriate sanctions for failure to comply.
C. Physical Safeguards: Ensure assigned security responsibilities, control access to media (e.g., diskettes, tapes, backups, disposal of data), protect against hazards and unauthorized access to computer systems, and secure workstation locations and use. The HSO may co-ordinate with the building security or facilities management personnel for this purpose.
D. Technical Safeguards: Establish access controls, emergency procedures, authorization controls, and data/entity access and authentication.

IV. ATTACHMENTS:

A. N/A

V. PURPOSE:

Partnership HealthPlan of California (PHC) is committed to ensuring the privacy and security of protected health information. In order to manage the facilitation and implementation of activities related to the privacy and security of protected health information, PHC will appoint and maintain an internal HIPAA Security Officer (HSO) position.

As required in 45 C.F.R. § 164.308(a)(2), Assigned Security Responsibility, the purpose of this policy is to establish how the HSO will serve as the focal point for security compliance-related activities and responsibilities, as listed below. The final responsibility for the implementation and maintenance of the security program must rest with one individual. In general, the HSO is charged with developing, maintaining, and implementing organizational policies and procedures, conducting educational programs, reviewing conduct of those assigned security responsibilities, and administering reviews relating to the

company's security program.

VI. POLICY / PROCEDURE:

A. Policy

PHC will identify the HIPAA Security Officer (HSO) who is responsible for the development and implementation of the policies and procedures required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and, specifically, Subpart C Security Standards for the protection of electronic protected health information (ePHI) of PART 164 – Security and Privacy.

B. Procedure

1. The HSO must demonstrate familiarity with the legal requirements relating to privacy and health care operations, as well as the ability to communicate effectively with and coordinate the efforts of technology and non-technology personnel. Information security will cover legal issues, hardware and software security, as well as physical security.
2. The current HIPAA Security Officer (HSO) is:
   - Kirt Kemp, Chief Information Officer
   - (707) 863-4103
   - 4665 Business Center Drive, Fairfield, CA 94534
   - kkemp@partnershiphp.org
3. In the event that the HSO needs to be replaced, the backup HSO will be the interim HSO. A search for a replacement HSO will be conducted and the position filled as soon as possible. Final determination of a new HSO will be made by the PHC Chief Executive Officer (CEO).
4. All workforce members will be made aware of the HSO identity, as well as the HSO's role and responsibilities. Any HSO changes will be promptly communicated.
5. The HSO leads in the development, awareness and enforcement of information security policies and procedures, measures and mechanisms to ensure prevention, detection, containment, and correction of security incidents. He/she will also ensure that the policy/procedure requirements comply with statutory and regulatory requirements regarding security of ePHI.
6. The HSO maintains security policies that include:
   a. Administrative Safeguards: Formal mechanisms for risk analysis and management, information access controls, and appropriate sanctions for failure to comply.
   b. Physical Safeguards: Ensure assigned security responsibilities, control access to media (e.g., diskettes, tapes, backups, disposal of data), protect against hazards and unauthorized access to computer systems, and secure workstation locations and use. The HSO may co-ordinate with the building security or facilities management personnel for this purpose.
   c. Technical Safeguards: Establish access controls, emergency procedures, authorization controls, and data/entity access and authentication.
7. The HSO maintains security procedures that include:
   a. Evaluation of compliance with security measures.
   b. Contingency plans for emergencies and disaster recovery.
   c. Security incident response process and protocols.
   d. Testing of security procedures, measures and mechanisms, and continuous improvement.
   e. Security incident reporting mechanisms and sanction policy.
   f. Proper documentation of security incidents and the responses to them.

8. The HSO ensures that appropriate security measures and mechanisms to guard against unauthorized access to electronically stored and/or transmitted patient data and protect against reasonably anticipated threats and hazards are in place. For example:
   a. Integrity controls.
   b. Authentication controls.
   c. Access controls.
   d. Encryption.
   e. Abnormal condition alarms, audit trails, entity authentication, and event reporting.
9. The HSO oversees the performance of on-going security monitoring of organization information systems
10. The HSO is responsible for directing periodic risk assessments as PHC systems or processes change or new ones are added. He/she will also be responsible for obtaining sign-off from appropriate management for acceptance of residual risks.
11. The HSO will ensure that functionality and gap analyses to determine the extent to which key business areas and infrastructure comply with statutory and regulatory requirements are conducted.
12. The HSO will oversee evaluation and recommendation of new information security technologies and counter-measures against threats to information or privacy.
13. The HSO ensures ongoing compliance through suitable training/awareness programs and periodic security audits.
14. The HSO serves as a resource regarding matters of informational security, and on a periodic basis, reports the status of information security activities to the CEO.
15. The HSO will ensure that security concerns have been addressed in system implementations including EMRs and any exchange of health information with patients and outside entities.
16. PHC shall require Business Associates to comply with the HIPAA security rule and all applicable PHC policies and procedures.

VII. REFERENCES:

A. Regulatory

45 C.F.R. §164.308 Administrative Safeguards

(a) A covered entity or business associate must, in accordance with § 164.306:
2. *Standard: Assigned security responsibility.* Identify the HIPAA Se**c**urity Officer who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

B. Internal

C. External

1. Health and Human Services – Office of Civil Rights, “Final Guidance on Risk Analysis”, (http://www.datamountain.com/wp-content/uploads/OCR_Risk-Analysis_Final_guidance.pdf)
2. National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1, "A Resource Guide for Implementing The HIPAA Security Rule" (http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf)

3. National Institute of Standards and Technology (NIST) Special Publication 800-30, "Risk Management Guide for Information Technology Systems" (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)
4. National Institute of Standards and Technology (NIST) Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems" (http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf)

VIII. DISTRIBUTION:
A. PowerDMS

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE: HIPAA Security Officer

X. REVISION DATES:
A. 08/01/2017
B. 07/05/2022

XI. PREVIOUSLY APPLIED TO:
A. N/A

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

Policy/Procedure Number: IT013				**Lead Department: IT**	
Policy/Procedure Title: Workforce Security				☐ **External Policy** ☒ **Internal Policy**	
Original Date: 05/01/2014			**Next Review Date:** ~~12/01/2023~~12/01/2024 **Last Review Date:** ~~07/05/2022~~12/01/2023		
Applies to:	☐ **Medi-Cal**		☒ **Employees**		
Reviewing Entities:	☐ **IQI**		☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**		☐ **EXECUTIVE**	☒ **COMPLIANCE**	☒ **DEPARTMENT**
Approving Entities:	☐ **BOARD**		☐ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO**	☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: ~~*Elizabeth Gibboney*~~*Sonja Bjork*				**Approval Date:** ~~08/22/2022~~08/22/2022	

I. RELATED POLICIES:

A. IT023 – Password Management
B. IT029 – Workstation Use
C. IT030 – Workstation Security
D. IT031 – Unique User Identification
E. CMP13 Permitted Use, Disclosure, and Minimum Use of Member Information

II. IMPACTED DEPTS:

A. N/A

III. DEFINITIONS:

A. Business Associate: As defined in 45 C.F.R. § 160.103, a business associate is a person or entity that performs certain functions that involve the use or disclosure of protected health information (PHI) on behalf of, or provides services, to a covered entity.
B. 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 PHC Board of Commissioners employed by or acting on the behalf of PHC.
C. Data Center – Dedicated space in a building, or a group of buildings used to house computer systems and associated components.

IV. ATTACHMENTS:

A. N/A

V. PURPOSE:

Partnership HealthPlan of California is committed to maintaining formal procedures to ensure that all workforce members have appropriate levels of access to electronic Protected Health Information (ePHI) and to prevent those personnel who do not have access to such information from obtaining access to ePHI. As such, Partnership HealthPlan of California will continually assess potential risks and vulnerabilities to individual health data in its possession, and develop, implement, and maintain appropriate security measures in accordance with 45 C.F.R. § 164.308, in general, and with 45 C.F.R. § 164.308(a)(3), Workforce Security, specifically.

Policy/Procedure Number: IT013		Lead Department: IT	
Policy/Procedure Title: Workforce Security		☐ **External Policy** ☒ **Internal Policy**	
Original Date: 05/01/2014		**Next Review Date: 12/01/202312/01/2024** **Last Review Date: 07/05/202212/01/2023**	
Applies to:	☐ **Medi-Cal**	~~Error! No text of specified style in document.~~ **~~Healthy Kids~~**	☒ **Employees**

VI. POLICY / PROCEDURE:

A. Policy
1. The policies and procedures stated herein apply to all ePHI created, maintained, or transmitted.
2. Workforce members, contractors, and Business Associates access only those areas (as determined by their Access Authorization Levels) and the applicable health information (as determined by their Personnel Clearance Levels) to which they are authorized.
3. The HIPAA Security Officer will designate specific individuals to perform the functions associated with establishing or removing Access Authorization and Personnel Clearance Levels as described in the procedures.
4. Workforce security review will be performed at least annually.

B. Procedure
1. Partnership HealthPlan of California's HIPAA Security Officer is responsible for determining the appropriate Access Authorization Levels and Personnel Clearance Levels for each position and maintaining a list detailing the level(s) of clearance and authorization levels for each workforce member [or classes of workforce members depending on their work function and the size of the organization].
2. ~~—~~Access Authorization Levels and Personnel Clearance Levels are role based and may be, depending on the size and nature of the workforce, established for groups or categories of workforce members. ~~such as: Physicians, Nurse Practitioners, Nurses, Medical Technicians, Administrative staff, etc.~~
3. ~~3.~~2. Information Technology Department, in coordination with the Human Resources Department will ensure that all workforce members be trained regarding their appropriate Access Authorization and Personnel Clearance Levels through orientation or repositioning within Partnership HealthPlan of California.
4. ~~4.~~3. To ensure minimum use necessary, when a workforce member changes roles within PHC, the workforce members direct report and/or department leadership shall submit a request via the IT Service Desk advising the role change.
5. ~~5.~~4. PHC shall disable a workforce member's network and application accounts, effectively on the last day of work or employment at PHC, regardless if the workforce members leaves voluntarily or involuntarily.
6. ~~6.~~5. To prevent those personnel who do not have access to such information from obtaining access to ePHI, the following protocols will be used to oversee and supervise all visitors, contractors or workforce members who must enter into an area for which they normally do not have Personnel Clearance or authorized access:
   a. Employees must meet visitors at the walk-up window to the reception area in the front lobby.
   b. All visitors must sign in at the front (lobby) reception desk, where a color-coded badge will be issued to them depending on their access level (business purpose).
   c. Visitors will have limited access and/or an escort, depending on business purpose.
   d. If an escort is required, that person responsible for ensuring that the appropriate level of ePHI is disclosed, depending on the access level.
7. ~~7.~~6. Partnership HealthPlan of California shall use and maintain time specifications for each access level, depending on job classification and business purpose (for visitors).
8. ~~8.~~7. The following areas are considered restricted. Depending on personnel role, the area may be granted as additional access.
   a. Data center
   b. Mailroom

Policy/Procedure Number: IT013		Lead Department: IT	
Policy/Procedure Title: Workforce Security		☐ **External Policy** ☒ **Internal Policy**	
Original Date: 05/01/2014		**Next Review Date: 12/01/202312/01/2024** **Last Review Date: 07/05/202212/01/2023**	
Applies to:	☐ **Medi-Cal**	~~Error! No text of specified style in document. **Healthy Kids**~~	☒ **Employees**

~~a.~~c. Network, Server, and UPS rooms

~~9.~~8. The HIPAA Security Officer may co-ordinate with HR, Legal or compliance functions as appropriate to perform this role effectively.

~~10.~~ When adding, modifying or canceling security clearance access upon repositioning of a workforce member, ~~IT~~ Facilities maintains record of the Personnel Clearance Level and Access Authorization List as appropriate.

Formatted: Indent: Left: 0.75", Hanging: 0.25", No bullets or numbering

VII. REFERENCES:

A. Regulatory Authority

45 C.F.R. §164.308 Administrative Safeguards

(a) A covered entity or business associate must, in accordance with § 164.306:

(3)(i)Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

1. Implementation specifications:
   a. Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
   b. Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

B. Internal

C. External

1. National Institute of Standards and Technology (NIST) Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems" http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
2. National Institute of Standards and Technology (NIST) Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems" http://csrc.nist.gov/groups/SMA/fisma/documents/Status-of-NIST-SP-800-26_v2.pdf
3. National Institute of Standards and Technology (NIST) Special Publication 800-12, Chapter 17 "An Introduction to Computer Security: The NIST Handbook" http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
4. National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1, "A Resource Guide for Implementing The HIPAA Security Rule"
5. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf

VIII. DISTRIBUTION:

A. PowerDMS

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE: All employees

X. REVISION DATES:

A. 01/02/2015

Policy/Procedure Number: IT013			Lead Department: IT
Policy/Procedure Title: Workforce Security			☐ **External Policy** ☒ **Internal Policy**
Original Date: 05/01/2014		**Next Review Date: 12/01/202312/01/2024** **Last Review Date: 07/05/202212/01/2023**	
Applies to:	☐ **Medi-Cal**	~~Error! No text of specified style in document.~~ **~~Healthy Kids~~**	☒ **Employees**

B. 06/24/2022
C. 07/05/2022
~~C.~~D. 12/01/2023

XI. PREVIOUSLY APPLIED TO:
A. N/A

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

Policy/Procedure Number: IT039				**Lead Department: IT**	
Policy/Procedure Title: Laptop Policy				☐ **External Policy** ☒ **Internal Policy**	
Original Date: 07/08/2015			**Next Review Date: 06/01/2024** **Last Review Date: ~~06/01/2023~~12/01/2023**		
Applies to:	☐ **Medi-Cal**		☒ **Employees**		
Reviewing Entities:	☐ **IQI**		☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**		☐ **EXECUTIVE**	☒ **COMPLIANCE**	☒ **DEPARTMENT**
Approving Entities:	☐ **BOARD**		☐ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO**	☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: *Sonja Bjork*				**Approval Date: ~~09/10/2023~~**	

Formatted: Font color: Red, Strikethrough

I. RELATED POLICIES:
- A. IT008 Risk Analysis and Management
- B. IT029 Workstation Use
- C. IT030 Workstation Security
- D. IT038 Media and Device Controls
- E. IT041 Storing Electronic Protected Information (ePHI)
- F. IT050 Remote Data Access
- G. FAC-304 Use of Company Property

II. IMPACTED DEPTS:
- A. All

III. DEFINITIONS:
- A. A laptop is a mobile device capable of performing all functions associated with a desktop computer, and has essential desktop hardware features including hard disks, CD drives, motherboards, displays (screens) and ports to connect mice, keyboards, external drives, network cabling, and printers. A laptop also can be mounted on a docking station.
- B. Security software is defined as full disk encryption, endpoint detection and response software and antivirus software and multifactor authentication (MFA).

IV. ATTACHMENTS:
- A. N/A

V. PURPOSE:

VI. Partnership HealthPlan of California (PHC) is committed to taking effective steps to implementing safeguards for all workstations that access sensitive data, restrict access to authorized users, and minimize or eliminate any potential risks and vulnerabilities to the electronic health information (ePHI) created, received, processed, transmitted or held by PHC employees or affiliates. PHC will continually assess potential risks and vulnerabilities to ePHI in its possession, and develop, implement, and maintain appropriate security measures in accordance with 45 C.F.R. § 164.308 in general, 45 C.F.R. § 164.308(1)(ii)(A), and 45 C.F.R. § 164.310(c) of the Health Insurance Portability and Accountability Act (HIPAA). The following laptop policy helps achieve this objective by establishing a standard for use that protects ePHI and sensitive company information, while providing enough flexibility to enable employees to complete work in the most efficient and accurate manner.

Policy/Procedure Number: IT039		Lead Department: IT
Policy/Procedure Title: Laptop Policy		☐ **External Policy** ☒ **Internal Policy**
Original Date: 07/08/2015	**Next Review Date: 06/01/2024** **Last Review Date: 06/01/202312/01/2023**	
Applies to:	☐ **Medi-Cal**	☒ **Employees**

POLICY / PROCEDURE:

A. Policy
1. Laptops are provided to PHC employees.
2. Laptops are intended to be used solely by the employee and should not be shared with family, friends or other employees.
3. All PHC laptops are encrypted using the Advanced Encryption Standard (AES) and deployed with security software.
4. Laptops are the property of PHC. It is the employee's responsibility to maintain the laptop in their care as best they can and to protect the laptop from theft. The employee may not physically alter or make any changes to the laptop without approval and assistance of I.T. Operations.
5. In the event that the laptop is lost or stolen, employee should report the loss immediately to IT Operations, ~~and~~ RAC, and your direct report or designee.
6. The employee is to promptly report any problems that arise to I.T. Operations team. All repairs are to be handled by the I.T. Operations team. The employee is not to take the laptop anywhere else for any kind of service or repair unless explicitly instructed to do so. They are not to attempt to repair or alter any part of the laptop.
7. The improper, careless, negligent, destructive, or unsafe use of equipment, as well as excessive or abusive use of a PHC issued laptop, can result in disciplinary action, up to and including termination of employment.
8. Emergency preparations should be made by employees and managers well in advance to allow remote work in emergency circumstances. This includes appropriate equipment needs (e.g. laptops). The I.T. department is available to review these equipment needs with employees and to provide support to employees in advance of emergency telework situations.
9. No ePHI or sensitive information shall be stored on laptop hard disks or any remote storage devices.
10. Laptop and laptop use is governed by PHC remote access policy; see IT050.

B. Procedure
1. All PHC employees will be issued only one type of computer.
2. Those employees who are issued laptops will turn over to I.T. all other PHC-owned computers (e.g. Micro PC, Desktop) that they are currently using.
3. All employees must sign a standard PHC remote access policy agreement (IT050) that applies to their terms of approval.
4. If an employee does not bring their laptop into the office, they shall be required to work with their manager to develop a plan for obtaining their laptop.
5. Upon leaving PHC the employee will return the laptop to HR or the Manager conducting the exit interview ~~the I.T. Operations team~~ on or before their final day of employment. HR and the ~~employee~~ manager will make arrangements to return the laptop to I.T. Operations.

Commented [KH1]: Policy request add per HR

~~VII.~~ **REFERENCES:**

A. Regulatory Authority

Formatted: Normal, No bullets or numbering

45 C.F.R. §164.308 Administrative Safeguards
A covered entity or business associate must, in accordance with § 164.306:
(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

Implementation specifications:
_Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
§ 164.310 Physical safeguards.

A Covered Entity or a Business Associate must, in accordance with § 164.306:
Standard: Workstation use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

B. External

1. National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1, "A Resource Guide for Implementing the HIPAA Security Rule" (http://csrc.nist.gov/publications/PubsSPs.htm l)

a. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 3 Final, "Recommended Controls for Federal Information Systems and Organizations" (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata 05-01-2010.pdf)

2. National Institute of Standards and Technology (NIST) Special Publication 800-53 A Rev 1, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans" (http://csrc.nist.gov/publications/nistpubs/800-53 A-rev 1 /sp800-53A-rev 1-final.pdf)

3. National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 1, "Computer Security Incident Handling Guide" (http://csrc.nist.gov/publications/nistpubs/800-6l-rev l/SP800-6l rev1.pdf)

4. National Institute of Standards and Technology (NIST) Special Publication "Guide to Computer Security Log Management" (http://csrc.nist.gov/publications/nistpubs/800- 92/SP800-92.pdf)

5. National Institute of Standards and Technology (NIST) Special Publication 800-122 Revision 3 Final, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" (http://csrc.nist.gov/publications/nistpubs/800- l 22/sp800-122.pdf)

6. National Institute of Standards and Technology (NIST) Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems" (http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf)

Policy/Procedure Number: IT039		Lead Department: IT
Policy/Procedure Title: Laptop Policy		☐ **External Policy** ☒ **Internal Policy**
Original Date: 07/08/2015		**Next Review Date: 06/01/2024** **Last Review Date: 06/01/202312/01/2023**
Applies to:	☐ **Medi-Cal**	☒ **Employees**

~~VIII.~~VII. **DISTRIBUTION**:
A. PowerDMS

~~IX.~~VIII. **POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE**: IT Operations

~~X.~~IX. **REVISION DATES:**
A. 07/14/2015
B. 07/05/2022
C. 06/01/2023
~~C.~~D. 12/01/2023

PREVIOUSLY APPLIED TO:
N/A

PARTNERSHIP HEALTHPLAN OF CALIFORNIA

POLICY/ PROCEDURE

Policy/Procedure Number: IT046				**Lead Department: IT**	
Policy/Procedure Title: 274 Provider Directory Data Submission and Issue Resolution Process				☐ **External Policy** ☒ **Internal Policy**	
Original Date: 05/09/2017			**Next Review Date: 09/01/2024** **Last Review Date: 09/01/2023**		
Applies to:	☐ **Medi-Cal**		☒ **Employees**		
Reviewing Entities:	☐ **IQI**		☐ **P & T**	☐ **QUAC**	
	☐ **OPERATIONS**		☐ **EXECUTIVE**	☒ **COMPLIANCE**	☒ **DEPARTMENT**
Approving Entities:	☐ **BOARD**		☐ **COMPLIANCE**	☐ **FINANCE**	☐ **PAC**
	☒ **CEO**	☐ **COO**	☐ **CREDENTIALING**	☐ **DEPT. DIRECTOR/OFFICER**	
Approval Signature: *Sonja Bjork*				**Approval Date:** ~~12/05/2023~~12/05/2023	

I. RELATED POLICIES:
A. N/A

II. IMPACTED DEPTS:
A. Information Technology
B. Provider Relations
C. Compliance
D. ~~Pharmacy~~

III. DEFINITIONS:
A. **274:** A Standard ASC X12 Electronic File for outbound Health Care Provider Directory
B. **DHCS:** Department of Health Care Services
C. **PDSRF:** Provider Data Submission Reconciliation Form
D. **EDI:** Electronic Data Interchange
E. **EIM:** Enterprise Information Management
F. **ITSI:** Information Technology Strategic Initiatives
G. **ETL:** Extract Transform and Load
H. **HCP:** Healthcare Plan Code

IV. ATTACHMENTS:
A. APL16-019
B. 274 Provider Network Companion Guide v1.3
C. Managed Care Provider Data Transition Planning v1.4
D. 274 Managed Care Provider Data FAQ v9.0
E. PACES Custom Error Messages 274 v1.2
F. PHC EDI Business Requirements Document

V. PURPOSE:
The purpose of the policy is to ensure that Partnership HealthPlan is meeting DHCS requirements for producing the 274 provider directory files for Medi-Cal and DMC ODS programs, and making every effort to convey quality data which accurately represents PHC's provider network. To document the workflow, roles and responsibilities for the 274 provider data file submissions and issue resolution process.

VI. POLICY / PROCEDURE:

A. **Monthly Submission Flow**

Formatted: Default Paragraph Font, Font: +Body (Calibri), 8 pt

Policy/Procedure Number: IT046		Lead Department: IT
Policy/Procedure Title: 274 Provider Directory Data Submission and Issue Resolution Process		☐ **External Policy** ☒ **Internal Policy**
Original Date: 05/09/2017	**Next Review Date: 09/01/2024** **Last Review Date: 09/01/2023**	
Applies to:	☐ **Medi-Cal**	☒ **Employees**

1. **Data Capture**

   a. External data for Medi-Cal Program from delegated entities will be collected by IT-EDI team by the 3rd Business day of the submission month.
      1) ~~Beacon~~ Carelon will send the 274 Production File by the 1st business day of the month.
      ~~2) Kaiser will send the 274 Production File by the 3rd business day of the month.~~
      ~~3)~~2) VSP will send the 274 Production File by the 1st business day of the month.

   b. External data sources include ~~Beacon~~Carelon, ~~Kaiser, MedImpact,~~ and VSP data.

   c. IT-EDW team will refresh the Provider Directory database at the end of the last calendar day of the month to ensure the most current data is captured.

   d. IT-EDI Team will generate and submit fourteen 274 files for Medi-Cal program incorporating both internal and external data by the 5th of each month.

      1) One file for each HCP/County Code.
         a) ~~Beacon~~ Carelon data will be repeated for all ~~fourteen~~ twenty-four counties.
         ~~b) Kaiser data will only be repeated for Solano, Marin, Napa, Sonoma, and Yolo.~~
         ~~c)~~b) VSP will be repeated for all ~~fourteen~~ twenty-four counties.

   e. IT-EDI Team will generate and submit one 274 file for DMC ODS program incorporating just internal data representing all DMC eligible counties by the 5th of each month.

2. **Rejection Error Resolution—Internal Data**

   a. IT-EDI Team will generate a hold report with the rejected errors and send to IT-EDW, Provider Relations, and Compliance teams by the 6th of the month.

   b. EIM and Provider Relations teams will work together to review and/or resolve any rejections or hold records which impact data integrity and/or representation of network adequacy.

   c. For error resolutions which are identified as needing to be resolved on the current submission month file the resolution must be complete by the 7th of the submission month.

   d. For errors which are identified as not critical to the current submission month file IT-EDI team will hold those records, and submit the 274 file without the impacted records.

   e. All errors, regardless of criticality, which are not resolved by the 7th of the submission month will be held to ensure timely submission of the 274 file.

   f. If an error is resolved past the 7th of the submission month it will be reported on the next month's file submission.

   g. If an error is resolved past the 7th of the submission month, but needs to be counted for the submission month file (ex. data missing for a site record in October, and PHC identifies the site needs to be included on the October file once corrected.)

1) Provider Relations must notify IT-EDI team of the request to resubmit the corrected record for the submission month it was held by the 3rd week of the current month. IT-EDI team will resubmit the 274 file(s) with the corrected record for the submission month it was held per DHCS retroactive resubmission guidelines (ex. October correction fixed in November, IT-EDI team notified by end of November, record is submitted in December, this file will replace the original October file for DHCS review.)
2) IT-EDI team will notify and work with DHCS regarding the corrected file submission and ensure that their team is aware of the retroactive resubmission.

h. If an issue is identified with the 274 file which requires analysis or programming changes for IT-EDI team then the issue should be submitted in Bug Zero to "PROJECT_274."

1) IT-EDI team will review the reported issue in Bug Zero and analyze the validity and impact of the error.
   a) If the issue reported is in relation to existing programming this will result in a service request ticket.
   b) If the issue reported is a request to add something new to the existing programming this will result in a WorkFront request.

2) IT-EDI team will respond to the issue submitter advising them to either open a service request ticket or a WorkFront request.

3. **Rejection Error Resolution—External Data**

a. IT-EDI Team will generate a hold report with the rejected errors and send this to each of our external delegates with Provider data.

1) A separate report will be generated for each of our external delegates
   a) One report for ~~Beacon~~Carelon, ~~Kaiser,~~ and VSP

2) Each report will be sent via email to the external delegates and will include PHC Internal Compliance-Regulatory Affairs team.

b. IT-EDI Team will coordinate error resolution with external delegates.

c. For error resolutions which are identified as needing to be resolved on the current submission month file the resolution must be complete by the 7th of the submission month.

d. For errors which are identified as not critical to the current submission month file IT-EDI team will hold those records, and submit the 274 file without the impacted records.

e. All errors, regardless of criticality, which are not resolved by the 7th of the submission month will be held to ensure timely submission of the 274 file.

f. If an error is resolved past the 7th of the submission month it will be reported on the next month's file submission.

g. If an error is resolved past the 7th of the submission month, but needs to be counted for the

submission month file (ex. data missing for a site record in October, and PHC identifies that the site needs to be included on the October file once corrected.)

1) Compliance ~~or Pharmacy~~ teams in conjunction with External delegate contact must notify IT-EDI team of the request to resubmit the corrected record(s) for the submission month it was held by the third week of the current month.

2) IT-EDI team will resubmit the 274 file(s) with the corrected record for the submission month it was held per DHCS retroactive resubmission guidelines (ex. October correction fixed in November, IT-EDI team notified by end of November, record is submitted in December, this file will replace the original October file for DHCS review.)

3) IT-EDI team will notify and work with DHCS regarding the corrected file submission and ensure that their team is aware of the retroactive resubmission.

h. If an issue is identified with the 274 file which requires analysis or programming changes for IT-EDI team then the issue should be submitted in Bug Zero to "PROJECT_274."

1) IT-EDI team will review the reported issue in Bug Zero and analyze the validity and impact of the error.
   a) If the issue reported is in relation to existing programming this will result in a Service Request ticket.
   b) If the issue reported is a request to add something new to the existing programming this will result in a WorkFront request.

2) IT-EDI team will respond to the Issue submitter advising them to either open a Service Request ticket or a WorkFront request.

4. **Final File Submission**
   a. IT-EDI Team will submit the final 274 file by the 10th of the month to DHCS.
   b. IT-EDI Team will hold any rejected error records which are not resolved by the 7th of the month, including internal and external data.
   c. Any corrections to this file received after the 7th of the month will be captured in a future month.

B. **Department Accountability and Expectations**
Departmental accountabilities and expectations vary and are outlined below:

1. **IT-EDI Team**
   a. Responsible for collecting, processing, and submitting all 274 Provider Directory data from both internal and external subcontracted delegates.
   b. Responsible for receiving and processing DHCS response reports.
   c. Responsible for generating and sharing Submission reports and Hold reports with respective Departments.
   d. Creating and sending the PDSRF reports to DHCS.
   e. Working with respective departments in resolving any reported issues.
   f. Working with DHCS on any outstanding issues/tasks and delay in processing or receiving responses.
   g. Updating and maintaining new edits and/or programming changes for future submissions as

required.

h. Participate in any 274 meetings i.e. report out on any issues, participate in group discussions, and contribute to analysis as needed.
i. Send the reviewed and approved monthly IT data certification report on the 274 submissions to RAC.

2. **IT-EDW Team**
   a. Responsible for extracting, transforming and loading provider data related to the 274 provider directory.
   b. Responsible for maintaining the structure and functionality of the Provider Directory database.
   c. Responsible for regular refresh of the Provider Directory database to ensure accurate and timely reporting.
   d. Responsible for reviewing and analyzing the Submission and Hold Reports in order to ensure data quality.
   e. Updating and maintaining programming for the ETL used in creating the Provider Directory database.
   f. Working with respective departments in resolving any reported issues.
   g. Participate in any 274 meetings i.e. report out on any issues, participate in group discussions, and contribute to analysis as needed.

3. **Provider Relations**
   a. Review monthly submission and hold reports for the 274 submission.
   b. Identify whether erroneous records should be corrected on the current month submission, require re-submission of the entire file retro-actively, or can be held on the current month and corrected on a future month submission.
      1) Communicate any issues on the hold report which require immediate correction on the current month submission to the IT-EDI team by the 7th of the submission report.
      2) Communicate any issues on the hold report which require retro-active file submission once the issue is corrected to the IT-EDI team by the 3rd week of the current month.
   c. Maintain code sets in Sugar system and communicate any 274 relevant changes to IT teams.
   d. Create and maintain operational workflows and policies in regards to inputting data relevant to the 274 file in the Sugar system.
   e. Working with respective departments in resolving any reported issues.
   f. Participate in any 274 meetings i.e. report out on any issues, participate in group discussions, and contribute to analysis as needed.

4. **Compliance**
   a. Review monthly submission and hold reports for the 274 submission.
   b. Identify whether any rejection errors require immediate correction from external delegates in order to correctly represent PHC's provider network.
   c. Work with external delegates in coordination with IT-EDI as an escalation point when required to resolve 274 related issues.
   d. Forward any relevant 274 communications from DHCS to 274 project team members.

C. **Internal/External Escalation**
1. The 274 Project team will meet on an ad hoc basis as needed to discuss any issues which require escalation.

Policy/Procedure Number: IT046		Lead Department: IT
Policy/Procedure Title: 274 Provider Directory Data Submission and Issue Resolution Process		☐ **External Policy** ☒ **Internal Policy**
Original Date: 05/09/2017	**Next Review Date: 09/01/2024** **Last Review Date: 09/01/2023**	
Applies to:	☐ **Medi-Cal**	☒ **Employees**

2. IT-EDI responds to issues/tasks related to delays in processing or receiving responses, and escalates to their DHCS point of contact, for resolution, when necessary.
3. Administration/Regulatory Affairs & Compliance researches regulatory inquiries related to 274 Provider Directory and escalates, as required, to our DHCS Contract Manager.

VII. REFERENCES:
A. N/A

VIII. DISTRIBUTION:
A. PowerDMS

IX. POSITION RESPONSIBLE FOR IMPLEMENTING PROCEDURE: ~~TBD~~

X. REVISION DATES:
A. 09/01/2023
~~A.~~B. 12/01/2023

PREVIOUSLY APPLIED TO:

2023 Regulatory Affairs and Compliance Dashboard

Category	Description	Q1	Q2	Q3	Q4	YTD	Comments
DELEGATION OVERSIGHT	**Annual Delegate / Subcontractor Audits**	**0 / 0**	**4 / 4**	**4 / 4**	**2 / 2**	**10 / 10**	
When PHC delegates administrative functions that it is required by contract or regulation to perform, PHC retains the ultimate responsibility for the performance of these functions and must monitor and evaluate the performance of these functions when performed by a delegate.	Quarterly percentage to demonstrate the total number of annual delegate/subcontractor audits completed within 30 days following the planned months, as defined by the audit calendar.	**#DIV/0!**	**100%**	**100%**	**100%**	**100%**	There were zero planned audits for Q1 2023
	Oversight of Delegate Reporting	**69 / 71**	**30 / 33**	**30 / 32**	**37 / 38**	**166 / 174**	
	Percentage of timely submissions of regulatory reports.	**97.2%**	**90.9%**	**94%**	**97%**	**95.4%**	
TRAINING	**Annual FWA Prevention Training**	**n/a**	**n/a**	**n/a**	**905 / 905**	**905 / 905**	
	Percentage of employees that have completed the annual FWA training. **Annual training released in Q4 2021**	**n/a**	**n/a**	**n/a**	**100.0%**	**100.0%**	
	Annual HIPAA Training	**n/a**	**n/a**	**n/a**	**904 / 904**	**904 / 904**	
	Percentage of employees that have completed the annual HIPAA training. **Annual training released in Q3 2021**	**n/a**	**n/a**	**n/a**	**100.0%**	**100.0%**	
	Annual Code of Conduct	**n/a**	**n/a**	**n/a**	**910 / 910**	**910 / 910**	
	Percentage of completed annual Code of Conduct employee attestations.	**n/a**	**n/a**	**n/a**	**100.0%**	**100.0%**	
REGULATORY REPORTING	**DHCS Reports Submitted Timely**	**56 / 56**	**53 / 54**	**47 / 48**	**51 / 52**	**207 / 210**	
Regulatory Affairs works collaboratively with all PHC departments to implement and track the timely submission of regulatory reporting requirements to PHC's governing agencies.	Percentage of regulatory reports submitted timely by RAC to DHCS with no missed due date per RAC Master Tracker and Regulatory Reporting Calendar.	**100.0%**	**98%**	**98%**	**98%**	**99%**	
	Report Acceptance Rate	**55 / 56**	**53 / 54**	**45 / 48**	**50 / 52**	**203 / 210**	
	Percentage of standard regulatory reports submitted by RAC and not rejected by DHCS for being incomplete, on the wrong template, or for other findings.	**98.2%**	**98.1%**	**94%**	**96%**	**96.7%**	
HIPAA REFERRALS	**Timely DHCS Privacy Notification Filings**	**3 / 3**	**6 / 7**	**4 / 4**	**5 / 6**	**18 / 20**	
Appropriate safeguards, including administrative policies & procedures, to protect the confidentiality of PHI and ensure compliance with HIPAA regulatory requirements.	Percentage of reportable notifications that PHC filed timely within applicable DHCS required timeframe. **Initial notice within 24 hours, initial PIR within 72 hours, and final PIR within 10 business days. If any deadline is missed, it will be counted as untimely.*	**100.0%**	**85.7%**	**100.0%**	**83%**	**90.0%**	Q1- 2 Delegate Breach Q2-Delegate reported a privacy case to DHCS outside of the required timeframe. 1 Delegate Breach Q3- 2 Contracted Provider Breach Q4- Delegate reported a privacy case to DHCS outside of the required timeframe
FWA REFERRALS	**Timely DHCS FWA Notifications**	**16 / 16**	**18 / 18**	**12 / 12**	**12 / 12**	**58 / 58**	
Regulatory Affairs oversees the Fraud, Waste and Abuse Prevention program intended to prevent, detect, investigate, report and resolve suspected and/or actual FWA in the PHC daily operations and interactions, whether internal or external.	Percentage of reportable notifications that PHC filed timely with DHCS within 10 business of discovery per contractual obligations.	**100.0%**	**100%**	**100%**	**100%**	**100%**	

***Threshold percentages for the above measures are as follows:**
≥ 95% = GREEN 90 - 94.9% = YELLOW < 90% = RED

CAP Tracker

*Please note that the above threshold percentages do not apply here