IMPERIAL COUNTY
Local Health Authority Commission

AGENDA

November 8th 2023
12:00 PM
1224 W State St. Ste. B
El Centro CA 92243

All supporting documentation is available for public review at https://chpiv.org

Committee Members	Representing	Present
Lee Hindman	LHA Chairperson – Joint Chambers of Commerce Nominee	
Yvonne Bell	LHA Vice-Chair & Finance Committee Vice-Chair – CEO, Innercare	
Dr. Carlos Ramirez	Finance Committee Chair – COO Unicare	
Mayra Widmann	Deputy CEO - Budget Fiscal.	
Dr. Unnati Sampat	LHA Commissioner – Imperial Valley Medical Society	
Dr. Allan Wu	LHA Commissioner – Innercare	

1. Call to Order — *Lee Hindman, Chairperson*

2. Roll Call — *Michelle S. Ortiz-Trujillo, SDHR*

3. Approval of Agenda
   a. Items to be pulled or added from the Information/Action/Closed Session Calendar
   b. Approval of the order of the agenda

4. Public Comment — *Lee Hindman, Chairperson*

   Public Comment is limited to items NOT listed on the agenda. This is an opportunity for members of the public to address the Committee on any matter within the Committee's jurisdiction. Any action taken as a result of public comment shall be limited to the direction to staff. When addressing the Committee, state your name for the record prior to providing your comments. Please address the Committee as a whole, through the Chairperson. Individuals will be given three (3) minutes to address the board.

CONSENT CALENDAR

5. Approval of Minutes from 10/04/2023

CLOSED SESSION — *Larry Lewis, CEO*

6. Pursuant to Welfare and Institutions Code § 14087.38 (n) Report Involving Trade Secret new product discussion (estimated date of disclosure, 01/2024)
   a. Update/Action on Contract with Health Net Community Solutions, Inc.

ACTION *Chairperson*

7. Report on actions taken in closed session.

8. Discussion/Action on Resolution for Treasurer Designation *Mark A. Southworth, CFO*

9. Discussion/Action on Resolution for CISSO Designation *Mark A. Southworth, CFO*

10. Discussion/Action on Resolution for Investment Account *Mark A. Southworth, CFO*

11. Discussion/Action on Resolution for Secondary Bank Account Establishment *Mark A. Southworth, CFO*

12. Discussion/Action regarding financial reports: *Mark A. Southworth, CFO*

    a. Fund Balance Report

        i. Through August 31, 2023

    b. Detailed Transaction Report

        i. Through August 31, 2023

    c. Revenue and Expenditures Report

        i. Through August 31, 2023

INFORMATION

13. Administrative Reports *Larry Lewis, CEO*

14. Other new or old business *Lee Hindman, Chairperson*

15. Commissioner Remarks *Lee Hindman, Chairperson*

Adjournment

Next Meeting: December 6th 2023

Impact of Safe Harbor Match

Cost	
2024 Salary Forecast	2,703,750
1% more match	**27,038**
Benefit	
Payroll Tax Risk	25,956

Notes

To have an employer match **not** as a Safe Harbor (full match up to 3%, half match up 1%) subjects us to a variety of ERISA regulations. We could have to pay our highly paid employees match as earned income, in which case we would need to pay payroll taxes, as well as the employee paying income taxes

Comparable Firm	Retirement max match/EC	Vesting
LACare		
CCAH	4.00%	None
IEHP	5.00%	5 years
CalOptima	Pension	CALPERS
Kaiser	6.25%	5 years
Kroger	4.00%	None
KPMG	2.50%	5 years
Walmart	6.00%	None
FedEx	8.00%	None
Bank Of America	5.00%	None
Amazon	4.00%	3 years
CVS	5.00%	None
US Avg (All Industries)	4.70%	
CHPIV Safe Harbor	4.00%	None

IMPERIAL COUNTY LOCAL HEALTH AUTHORITY
dba Community Helath Plan of Imperial Valley
Year to Date P&L Variance
1/1/2023 to 9/30/2023

	Year To Date September Forecast	Year To Date September Actual	Variance	Explanation
REVENUE				
Capitation Revenue	1,061,928	1,081,068	19,140	
Other Revenue		1,947,414	1,947,414	Profit Share
Reinsurance Revenue				
Interest Income	63,779	261,262	155,779	Higher than expected interest rates
TOTAL REVENUE	1,125,707	3,289,743	2,164,036	
HEALTH CARE COSTS				
ADMINISTRATIVE EXPENSE				
Salaries	1,215,696	850,517	-365,179	Hiring took longer than expected for many positions
Benefits	237,466	46,104	-191,362	Health Insurance Expense may be misclassed
Total Labor Costs	1,453,162	896,621		
Benefits % of Salaries	20%	5%		Our sister plans run around 35%
Furniture & Equipment				
Contract Servicse/Marketing/Network Rent	1,349	107,448	106,099	
Consulting, Audit, Legal, Audit	1,073,725	794,373	-279,352	
Office Expense	141,274	82,954	-58,320	
Total Administrative Exense	1,216,348	984,775	-231,573	
Non-Operating	200,000	200,000		
Excess Revenues from Operations	(1,543,803)	613,974	2,157,777	Profit Share and Hiring Schedule

COMMUNITY HEALTH PLAN OF IMPERIAL VALLEY

Human Resources
1224 West State Street
Suite B
El Centro CA 92243

Community Health Plan of Imperial Valley Staff

Dear Staff Member,

We are issuing this notice to inform you of the changes we have made to our current retirement plan. Please see changes below.

We're enhancing our retirement plan in two ways for 2024:

1. We're moving to opt-in, where an employee who makes no decision will not contribute to retirement.
2. We're adjusting the employer matching agreement to be equal match on the first 3% and half match on the next two percent.
    a. For example an employee contributing 5% would get the full employer match of 3+(1/2)*2=4%

This is a collaborative effort on behalf of your Finance and Human Resources Departments. Should you have any questions please contact mortiz@chpiv.org.

Best Regards,

Finance and Human Resources Department

IMPERIAL COUNTY
Local Health Authority Commission

1. Investment Policy

Situation	I'm requesting the board approve an investment policy
Background	California law requires all independent government entities have an investment policy
Assessment	We need an investment policy to operate as an independent entity from the Imperial County. We should have this in place by 1/1/2024.
Recommendation	We should adopt a simple policy that meets the State requirements and gives the board appropriate vision and control of the investment decisions

2. Treasurer designation for Mark Southworth

Situation	I'm asking the board to name me Treasurer
Background	California Law requires all public entities to designate a Treasurer who is given a variety of rights and responsibilities in the Investment Policy
Assessment	This designation is usually given to the CFO. Sometimes additional responsibilities and privileges are given to the treasurer. We should have this in place by 1/1/2024
Recommendation	Grant the Treasurer designation to Mark, but with no additional rights or responsibilities

3. City National Bank for restricted deposit and explore investment manager options

Situation	I'm asking for permission to establish a client relationship with City National Bank and create two accounts: a Knox Keene restricted deposit, and a governmental investment account
Background	It was a challenge to establish the First Foundation restricted deposit account and the possibility of First Foundation closing the account presents a clear business risk to us. The investment manager requirement comes from the state proscribed Investment Policy. Our sweep is performing well so far this year, but in more normal economic circumstances we will want a more diversified portfolio. It's my read of the Investment Policy that as we separate from the County the diversification becomes mandatory
Assessment	In my conversations with our LHPC sister plans several recommended City National as a one-stop-shop for handling both the restricted deposit, and the investment management
Recommendation	Grant authority to Mark to set up the second restricted deposit account and begin exploring both City National and Chase as investment managers.

4. **Chase second operating account**

Situation	Prudent financial management calls for separating our reserve funds from our operations expense account.
Background	We're currently operating primarily out of a combination of First Foundation and the County fund. Both of these entities are unsatisfactory: the county is unreliable in making payments, and First Foundation lacks the extensive financial controls of Chase.
Assessment	We should be operating out a highly responsive and reliable bank that offers the appropriate financial controls. Chase meets those criteria. Other banks may as well, but we already have a relationship with Chase. We have a large checking account at Chase, but given it's size it presents a security risk if we share the ACH instructions too widely.
Recommendation	Open the second account for operations at Chase

5. **CISO Designation**

Situation	We need to establish a Chief Information Security Officer
Background	A requirement of HIPAA is that we have a board designated Chief Information Security Officer (CISO). This not a specific C-Suite position, but a designation a person who all security breaches are reported, and who reports them upstream to our regulators.
Assessment	This could be any long-term employee. It's most often assigned to either the Chief Information/Technology Officer or a senior leader in Compliance.
Recommendation	Alejandro is the best candidate for this position as he will be the one most actively monitoring our information security and appears to be a long term employee.

6. Retirement plan adjustment

Situation	We need to make an adjustment to our retirement plan to meet the benefits promised to existing employees
Background	We promised a 3% retirement plan employer contribution match to most employees in their offer letter. At implementation we discovered that, as a "top heavy" organization the 3% match would likely run afoul of the ERISA non-discrimination provisions if non-highly compensated employees do not save at a similar rate to highly compensated employees. This would cause the employer contributions to be returned from the retirement plan to employees at the end of the year as regular taxable income and incur regular payroll taxes for CHPIV. As a stopgap for 2023 we made the 3% a discretionary employer profit share contribution, rather than a match.
Assessment	Employer matches are a very effective incentive to encourage employees to save for retirement. ERISA has a specific exemption for top-heavy organizations like us called the Safe Harbor contribution. If we adopt the proscribed Safe Harbor 3% full match and 1% half-match we will not be subject to ERISA non-discrimination testing. If

	all employees take advantage of the change, we would incur an extra $27,000 of employee benefit expense in 2024. The 4% total match would still put us on the low end of comparable employers.
Recommendation	We should adopt the standard Safe Harbor contribution match.

RESOLUTION OF THE IMPERIAL COUNTY LOCAL HEALTH AUTHORITY AUTHORIZING ESTABLISHMENT OF A BANK ACCOUNT.

RESOLUTION NO._____

WHEREAS, the Local Health Authority ("LHA") Commission is committed to the entity's autonomous operation as pursuant to section 8.03.070 of the Codified Ordinances of the County of Imperial and within section 14087.38 of the Welfare and Institutions Code.

WHEREAS, on October 11, 2022, the LHA Commission approved by majority vote the establishment of a personnel system independent of the County of Imperial and to carry out those functions, the LHA must obtain a bank account independent of the County of Imperial's fiscal operation.

WHEREAS, a proposal to open a second account with Chase Bank was placed before the Commission on November 13th 2023 and after discussions a majority vote authorized the opening of said bank account for the sole purpose of Operating Expenses.

NOW, THEREFORE, the LHA resolves as follows:

(1) The Recitals set forth above are true and correct and are incorporated into this Resolution by this reference.

(2) The legal name of the entity is as submitted on form SF-45, "Imperial County Local Health Authority," shall be assigned as the name on the bank account.

(3) The account shall be opened with Chase Bank.

(4) The authorized signer's privilege is conveyed to those that hold the position of
   a. Mr. Lee Hindman, Chairperson
   b. Mrs. Yvonne Bell, Vice-Chair
   c. Larry Lewis, Chief Executive Officer
   d. Mark A. Southworth, Chief Financial Officer

(5) The staff of LHA are hereby authorized and directed to take all actions necessary to carry out the intent and purpose of this Resolution.

(6) This Resolution shall take effect immediately upon its adoption.

PASSED AND ADOPTED by the Local Health Authority, County of Imperial, State of California, this _____day of _____ 2021, by the following roll call vote:

_____.

_____
Dr. Adolphe Edward,
Chairman

ATTEST:

_____
Lee Hindman
Vice-Chair

RESOLUTION OF THE IMPERIAL COUNTY LOCAL HEALTH AUTHORITY AUTHORIZING WIRE TRANSFERS.

RESOLUTION NO._____

WHEREAS the Local Health Authority ("LHA") Commission is committed to the entity's autonomous operation as pursuant to section 8.03.070 of the Codified Ordinances of the County of Imperial and within section 14087.38 of the Welfare and Institutions Code.

WHEREAS, on November 13th 2023, the LHA Commission approved by majority vote the direction to staff to establish an Investment Account.

WHEREAS, on November 13th 2023, the LHA Commission approved by majority vote the direction to staff to establish an Investment Account Manager.

WHEREAS, to continue business operations in a timely manner the Imperial County local Health Authority is authorizing any of the below mentioned to complete these tasks.

NOW, THEREFORE, the LHA resolves as follows:

(1) The Recitals set forth above are true and correct and incorporated into this Resolution by this reference.

(2) The Investment Account Manager's privilege is conveyed to those that hold the position of
a.

(3) The staff of LHA are hereby authorized and directed to take all actions necessary to carry out the intent and purpose of this Resolution.

(4) This Resolution shall take effect immediately upon its adoption.

PASSED AND ADOPTED by the Local Health Authority, County of Imperial, State of California, this _____day of _____ 2023, by the following roll call vote:

_____.

_____
Mr. Lee Hindman,
Chairman

ATTEST:

_____
Yvonne Bell

Vice-Chair

RESOLUTION OF THE IMPERIAL COUNTY LOCAL HEALTH AUTHORITY AUTHORIZING WIRE TRANSFERS.

RESOLUTION NO._____

WHEREAS the Local Health Authority ("LHA") Commission is committed to the entity's autonomous operation as pursuant to section 8.03.070 of the Codified Ordinances of the County of Imperial and within section 14087.38 of the Welfare and Institutions Code.

WHEREAS, on November 13th 2023, the LHA Commission approved by majority vote the establishment of a Chief Information Security Officer for the Local Health Authority to be assigned to the Information Technology and Security Analyst.

WHEREAS, to continue business operations in a timely manner the Imperial County local Health Authority is authorizing any of the below mentioned to complete these tasks.

NOW, THEREFORE, the LHA resolves as follows:

(1) The Recitals set forth above are true and correct and incorporated into this Resolution by this reference.

(2) The Chief Information Security Officer's privilege is conveyed to those that hold the position of
   a. Ignacio Alejandro Franco, Information Technology and Security Analyst.

(3) The staff of LHA are hereby authorized and directed to take all actions necessary to carry out the intent and purpose of this Resolution.

(4) This Resolution shall take effect immediately upon its adoption.

PASSED AND ADOPTED by the Local Health Authority, County of Imperial, State of California, this _____day of _____ 2023, by the following roll call vote:

_____.

_____
Mr. Lee Hindman,
Chairman

ATTEST:

_____
Yvonne Bell
Vice-Chair

RESOLUTION OF THE IMPERIAL COUNTY LOCAL HEALTH AUTHORITY AUTHORIZING FUNDING OF REQUIRED RESTRICTED DEPOSIT OF $300,000.

RESOLUTION NO._____

WHEREAS, the Local Health Authority ("LHA") Commission is committed to the entity's autonomous operation pursuant to section 8.03.070 of the Codified Ordinances of the County of Imperial and within section 14087.38 of the Welfare and Institutions Code.

WHEREAS, on October 11, 2021, the LHA Commission voted to give direction to LHA staff to prepare an application for a Knox-Keene license from the Department of Managed Health Care.

WHEREAS, to carry out such Knox-Keene application and to operate the Knox-Keene entity once licensed, the LHA is required to fund a restricted deposit account in the amount of $300,000, and assign said account to the Director of the Department of Managed Health Care. A complete and executed Form 1300.76.1 must be completed in order to accomplish the assignment.

WHEREAS, on November 13th 2023, the LHA Commission voted to give direction to the Chief Financial Officer and staff to set up a secondary restricted deposit account.

NOW, THEREFORE, the LHA resolves as follows:

(1) The Recitals set forth above are true and correct and incorporated into this Resolution by this reference.

(2) The legal name of the entity as submitted on form SF-45 is, "Imperial County Local Health Authority," shall be assigned as the name on the bank account.

(3) The staff of LHA are hereby authorized and directed to take all actions necessary to carry out the intent and purpose of this Resolution.

(4) This Resolution shall take effect immediately upon its adoption.

PASSED AND ADOPTED by the Local Health Authority, County of Imperial, State of California, this _____day of _____ 2023, by the following roll call vote:

_____.

_____
Lee Hindman,
Chairman

ATTEST:

_____
Yvonne Bell
Vice-Chair

RESOLUTION OF THE IMPERIAL COUNTY LOCAL HEALTH AUTHORITY AUTHORIZING WIRE TRANSFERS.

RESOLUTION NO._____

WHEREAS the Local Health Authority ("LHA") Commission is committed to the entity's autonomous operation as pursuant to section 8.03.070 of the Codified Ordinances of the County of Imperial and within section 14087.38 of the Welfare and Institutions Code.

WHEREAS, on November 13th 2023, the LHA Commission approved by majority vote the establishment of a treasurer for the Local Health Authority naming the Chief Financial Officer for the position.

WHEREAS, , to continue business operations in a timely manner the Imperial County local Health Authority is authorizing any of the below mentioned to complete these tasks.

NOW, THEREFORE, the LHA resolves as follows:

(1) The Recitals set forth above are true and correct and incorporated into this Resolution by this reference.

(2) The Treasure's privilege is conveyed to those that hold the position of
   a. Mark A. Southworth, Chief Financial Officer.

(3) The staff of LHA are hereby authorized and directed to take all actions necessary to carry out the intent and purpose of this Resolution.

(4) This Resolution shall take effect immediately upon its adoption.

PASSED AND ADOPTED by the Local Health Authority, County of Imperial, State of California, this _____day of _____ 2023, by the following roll call vote:

_____.

_____
Mr. Lee Hindman,
Chairman

ATTEST:

_____
Yvonne Bell
Vice-Chair

HIPAA Privacy Training

Training Material

Quiz Submission Due: December 11, 2023

Community Health Plan OF IMPERIAL VALLEY

Table of Contents

I. Objectives 3

II. Projecting 3

III. Privacy & Security 3

IV. Key Terms 3

V. Identifiers 4

VI. Member Rights 4

VII. Accessing PHI 5

VIII. Minimum Necessary Rule 5

IX. Your Role in Projecting 5

X. Secure Emails 6

XI. Oversight 6

XII. Disclaimer 7

XIII. APPENDIX 7

I. Objectives

A. Protecting Privacy and Security
B. Review key terms and definitions
C. Understand when it is appropriate to access Member/Patient information – "Minimal Necessity Rule"
D. Member Rights
E. Understand your role for identifying and reporting HIPAA Privacy and Security issues

II. Projecting

A. Members/Patients routinely share personal information with health care providers. If the confidentiality of this information is not protected, trust in the physician-patient and healthcare relationship would be affected.

III. Privacy and Security

A. Health care entities must take steps to ensure that Member/Patient protected health information (PHI) is not viewed by anyone without "a business need to know," and is not stolen, lost, or accidentally destroyed.
B. Posting ANY member information or photos even without names may lead to termination, fines and jail time

IV. Key Terms

A. What is HIPAA?
    1. Health Insurance Portability and Accountability Act of 1996 is a federal law that required the creation of national standards to protect patient health information (PHI) from being disclosed without the patient's consent or knowledge.
B. What is PHI?
    1. Protected Health Information (PHI) is information that relates to a member's/patient's past, present or future physical or mental health care or condition, including any payment for physical or mental health care, as well as any associated personally identifying information (PII)**
    2. ** PII - A general term used to describe any form of sensitive data that could be used to identify or contact an individual. For example, any payment or authentication information (i.e., mother's maiden name) is considered PII. When PII is used in connection with a member/patient's physical or

mental health care or condition or condition or payment for said care, PII becomes PHI

C. What Types of PHI are Protected?
    1. Paper Records
    2. Electronic Records
    3. Oral Communication
    4. Fax/Email documents
    5. *Any* information that can identify the member and is related to the person's past, present or future physical or mental health condition
    6. Anything associated with healthcare services or treatment

V. Identifiers

A. The Department of health care services (DHCS) lists the 18 HIPAA identifiers that are considered Personally identifiable:
    1. Names
    2. Address / Geographic area
    3. All elements of dates such as Date of Birth, Admit / discharge date, Date of Death
    4. Telephone numbers
    5. Fax numbers
    6. Email addresses
    7. Social Security numbers
    8. Medical Records numbers
    9. Health plan beneficiary numbers
    10. Account numbers
    11. Certificate/license numbers
    12. IN and serial numbers, including license plate numbers
    13. Device identifiers and serial numbers
    14. Web URLS
    15. IP address numbers
    16. Biometric identifiers, including finger and voice prints
    17. Full face photographic images and any comparable images
    18. Any other unique identifying number, characteristic, or code, except as permitted

VI. Members Rights

A. **Mandated by HIPAA, members have the right to:**
    1. Receive the Notice of Privacy Practice
    2. Access their medical records
    3. Request amendments to their medical records
    4. An accounting of disclosures of their medical records
    5. Request restrictions on release of PHI
    6. File a complaint

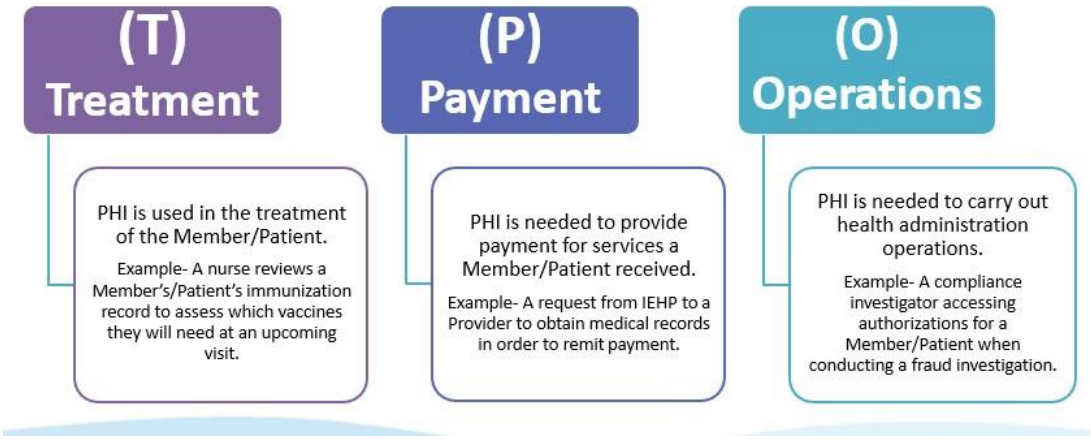
B. Compliance Policy

1. Notice of Privacy Practices CMP-012

VII. Accessing PHI

A. The law allows access and disclosure of Member/Patient PHI when a request or need for information falls under Treatment, Payment or Operations (TPO).

B. Access to PHI without member/patient authorization is not limited to TPO (see 45 CFR 164.502).



VIII. Minimum Necessary Rule

A. **Understand when it is appropriate to access Member/Patient information**

B. **"Minimum Necessary" Rule**

1. Clinical staff, physicians and employees are required to access only the information *they need to do their job* for treatment, payment or healthcare operations (TPO)
2. Release of PHI without a signed Authorization Form is not permitted
3. Access to your family/friends' records is not permitted without a signed Authorization Form from the member
4. 45 CFR 165.500 seq

IX. Your Role in Protecting

A. Only access information your job REQUIRES for TPO (Treatment, Payment, Healthcare Operations)

B. Prior to release of PHI, ensure Authorization Form is obtained (as needed for compliance with the Privacy Rule)

C. If transmitting PHI electronically, ensure that you are sending the transaction through a secure portal or through a secure email

1. If faxing is required, a cover sheet can be sent to a physician office or other health care facility's fax machine that is within a secure location. Before faxing, make sure to:
2. Confirm the fax number prior to sending

3. Send fax to approved fax numbers, or make sure the recipient is waiting by the machine to receive the fax
4. If sent to an inappropriate fax number, report the matter to your supervisor immediately

D. Do not share member information in open areas where you can be overheard by others
E. Lock your computer *every* time you walk away, and/or log off at the end of the day
F. Do not share or disclose member information with family, friends or co-workers
G. Do not email, post or text (including photos) anything that can identify a member
H. Know the permission level granted by the member in order to leave a HIPAA-compliant voice message
I. Know how and where to dispose of all PHI – shred, locked bins, etc.
J. PROMPTLY REPORT MEMBER PRIVACY INCIDENTS to your supervisor, privacy officer per your company policy
K. Compliance Policy
    1. Notice of Privacy Practices CMP-0012

X. Secure Emails

A. Securing Emails is mandatory for all HIPAA protected information going outside Community Health Plan of Imperial Valley
B. Process for Securing Emails:
    1. Microsoft 365 automatically encrypts all emails sent within CHPIV and servers that allow standard encrypted emails
    2. To protect any sensitive information when sending to external recipient's subject line states "Encrypt It"
    3. After sending the email, an email is received confirming the message was encrypted.
    4. The recipient will receive an email with instructions on how to sign into Advanced Email Security to view and respond to the encrypted message. The email expires after 15 days, and the recipient cannot forward or save it (but they can download attachments from the email).

XI. Oversight

A. Oversight of HIPAA and security is:
    1. Compliance Policy
        a. *Excerpt:* Breach Notification CMP-011
            i. ***Procedure****:* Anonymously reporting HIPAA Violations. Potential breaches may be reported

anonymously to CHPIV through the Compliance Hotline (800-919-4947)

XII. Disclaimer

A. This course was prepared as a service and is not intended to grant rights or impose obligations. This course may contain references or links to statutes, regulations or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. Readers are encouraged to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

XIII. APPENDIX

A. Compliance Policy
    1. Breach Notification CMP-011
    2. Notice of Privacy Practices CMP-012

	Breach Notification	CMP-011
	Department	Compliance
	Functional Area	Compliance
	Impacted Delegate	☒ Subcontractor ☐ NA

DATES			
Policy Effective Date	10/9/2023	Reviewed/Revised Date	
Next Annual Review Due	10/9/2024	Regulator Approval	8/25/2023

APPROVALS		
Internal		**Regulator**
Name	Elysse Tarabola	☒ DHCS ☐ NA ☐ DMHC
Title	Chief Compliance Officer	

ATTACHMENTS

- NA

AUTHORITIES/REFERENCES

- CHPIV Contract with the Department of Health Care Services (DHCS) for Medi-Cal
- CHPIV Compliance Plan
- HIPAA Breach Notification Rules, 45 CFR §164.400 et seq.
- HHS Commentary Re: Breach Notification Rules, 74 FR 42740 (Aug. 24, 2009) and 78 FR 5638 (Jan. 25, 2013)
- HHS Guidance for Securing Protected Health Information, 74 FR 42741 (Aug. 24, 2009); also available at www.hhs.gov/ocr/privacy.
- Information Practices Act at California Civil Code section 1798.3(a)

HISTORY

Revision Date	Description of Revision
10/9/2023	Policy creation

I. OVERVIEW

A. The purpose of this policy is to enable CHPIV to comply with applicable state and federal laws and regulations governing notice to affected persons in the event of a breach of Member privacy.

B. Violation of this Policy may result in disciplinary action, up to and including termination of employment and/or contract, civil and/or criminal action, and other legal and other remedies available to CHPIV.

II. POLICY

A. The Senior Director of Compliance serves as CHPIV's Privacy Officer.

B. CHPIV workforce members will maintain the privacy and security of MEMBERS' PROTECTED HEALTH INFORMATION (PHI) consistent with CHPIV's policies, procedures, and applicable laws and regulations. CHPIV will notify the Member, U.S. Department of Health and Human Services (HHS), DEPARTMENT OF HEALTH CARE SERVICES (DHCS), and in some cases, local media if there is a breach of unsecured PHI unless CHPIV can demonstrate a low probability that the information has been compromised.

C. This Policy applies to all CHPIV workforce members, including CHPIV administration, medical staff, clinical and administrative workforce members, volunteers, and CHPIV's business associates.

D. Breaches of PHI. This policy applies only if there is a breach of a Member's individually identifiable health information. For purposes of this policy, a breach is presumed if there is an unauthorized access, acquisition, use or disclosure of unsecured PHI unless, (1) CHPIV can demonstrate that there is a low probability that the information was compromised based on a risk assessment of certain factors described below, or (2) the situation fits within one of the following exceptions to the breach notification rule:

1. Any unintentional acquisition, access or use of PHI by a CHPIV workforce member or a person acting under CHPIV's authority if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in violation of the HIPAA PRIVACY RULES.
2. Any inadvertent disclosure by a person who is authorized to access PHI at CHPIV to another person authorized to access Member information at CHPIV and the Member information disclosed is not further used or disclosed in violation of the HIPAA PRIVACY RULES.
3. A disclosure of PHI if CHPIV has a good faith belief that the person to whom the disclosure was made would not reasonably have been able to retain such information.
4. The use or disclosure involves PHI that has been "secured" according to standards published by HHS. Currently, this only applies to electronic Member information that has been properly encrypted consistent with standards published by HHS. HHS will publish future guidance for securing Member information on its website, https://www.hhs.gov/hipaa/index.html. (45 CFR § 164.402)

III. PROCEDURE

A. Mitigating Potential Breaches. If CHPIV workforce members improperly access, acquire, use or disclose PHI and immediate action may cure or mitigate the effects of such use or disclosure, CHPIV workforce members should take such action. For example, if CHPIV workforce members improperly access or acquire PHI, they should immediately stop, close,

and/or return the information. If CHPIV workforce members mistakenly disclose PHI to the wrong person, they should immediately request the return of the information and confirm that no further improper disclosures will be made. If the potential breach is significant or requires further action to mitigate its effects, CHPIV workforce members should immediately contact their supervisor and the Senior Director of Compliance for assistance and direction.

B. Reporting Potential Breaches to the Senior Director of Compliance. CHPIV workforce members shall immediately report any suspected breach of PHI in violation of HIPAA PRIVACY RULES or CHPIV's privacy policies to the Senior Director of Compliance. Failure to timely report suspected breaches may result in sanctions as described below.

C. Anonymously reporting HIPAA Violations. Potential breaches may be reported anonymously to CHPIV through the Compliance Hotline (800-919-4947)

D. Investigating Potential Breaches. The Compliance department shall promptly investigate any reported privacy breach or related Member complaint to determine whether there has been a "breach" of PHI as defined above, and if so, how notice should be given. To determine whether a breach has occurred, the Compliance department shall consider:

1. Whether the alleged breach involved PHI.
2. Whether the alleged breach violates the HIPAA PRIVACY RULES. Disclosures that are incidental to an otherwise permissible use or disclosure (e.g., a Member overhears a customer service representative speaking with another MEMBER, or sees information about another MEMBER on a whiteboard or sign-in sheet) does not violate the privacy rule so long as CHPIV implemented reasonable safeguards to avoid improper disclosures. (45 CFR § 164.502(a)(1)(iii))
3. Whether there is a low probability that the PHI has been compromised considering relevant factors, including at least the following: (1) the nature and extent of the information involved; (2) the unauthorized person who used or received the information; (3) whether the information was actually acquired or viewed; and (4) the extent to which the risk to the information has been mitigated. (45 CFR § 164.402)
4. Whether the alleged breach fits within one of the exceptions identified in Section II.3 (a)-(d), above. (45 CFR § 164.402) The Senior Director of Compliance shall document his or her investigation and conclusions, including facts relevant to the risk assessment. (45 CFR §§ 164.414 and 164.530)

E. Notice—In General. If the Compliance department determines that a breach of unsecured PHI has occurred, the Senior Director of Compliance shall notify the MEMBER, HHS, DHCS, and the media (if required) consistent with this policy and the requirements of 45 CFR §§ 164.404 et seq. Any notice provided pursuant to this policy must be approved and directed by the Senior Director of Compliance and/or CHPIV senior leadership. No other CHPIV workforce members are authorized to provide the notice required by this policy unless expressly directed by the Senior Director of Compliance .

F. Notice to MEMBERS. If a breach of PHI has occurred, the Compliance department shall notify the affected MEMBER(S) without unreasonable delay and in no case later than 60 days after the breach is discovered. The notice shall include to the extent possible: (1) a brief description of what happened (e.g., the date(s) of the breach and its discovery); (2) a description of the types of information affected (e.g., whether the breach involved names, social security numbers, birthdates, addresses, diagnoses, etc.); (3) steps that affected MEMBERS should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what CHPIV is doing to investigate, mitigate, and protect against further harm or breaches; and (5) contact procedures for affected persons to ask questions

and receive information, which shall include a toll-free telephone number, e-mail address, website, or postal address at which the person may obtain more information. The notice shall be written in plain language. (45 CFR § 164.404)

1. Notice by Mail or Email. The Compliance department shall notify the MEMBER by first class mail to the Member's last known address. If the MEMBER agrees, the notice may be sent by e-mail. The notice may be sent by one or more mailings as information is available. (45 CFR § 164.404(d))
2. Substitute Notice. If CHPIV lacks sufficient contact information to provide direct written notice by mail to the MEMBER, the Compliance department must use a substitute form of notice reasonably calculated to reach the MEMBER. (45 CFR § 164.404(d))
    a. Fewer than 10 affected MEMBERS. If there is insufficient contact information for fewer than 10 affected MEMBERS, the Compliance department shall provide notice by telephone, e-mail, or other means. If the Compliance department lacks sufficient information to provide any such substitute notice, the Compliance department shall document same. (45 CFR § 164.404(d)(2)(i))
    b. 10 or more affected MEMBERS. If there is insufficient contact information for 10 or more affected MEMBERS, the Compliance department shall do one of the following after consulting with CHPIV senior leadership: (1) post a conspicuous notice on the home page of CHPIV's website for 90 days with a hyperlink to the additional information required to be given to individuals as provided above; or (2) publish a conspicuous notice in major print or broadcast media in the area where affected MEMBERS reside. The notice must include a toll-free number that remains active for at least 90 days so individuals may call to learn whether their PHI was breached. (45 CFR § 164.404(d)(2)(ii))
3. Immediate Notice. If the Senior Director of Compliance believes that PHI is subject to imminent misuse, the Senior Director of Compliance may provide immediate notice to the MEMBER by telephone or other means. Such notice shall be in addition to the written notice described above. (45 CFR § 164.404(d)(3))

G. Deceased MEMBER; Notice to Next of Kin. If the MEMBER is deceased and CHPIV knows the address for the Member's next of kin or personal representative, the Compliance department shall mail the written notice described above to the next of kin or personal representative. If the CHPIV does not know the address for the next of kin or personal representative, CHPIV is not required to provide any notice to the next of kin or personal representative. The Compliance department shall document the lack of sufficient contact information. (45 CFR § 164.404(d)(1))

H. Notice to Regulators.

1. Notice to HHS. If the Compliance department determines that a breach of PHI has occurred, the Compliance department shall also notify HHS of the breach as described below.
    a. Fewer than 500 Affected MEMBERS. If the breach involves the PHI of fewer than 500 MEMBERS, the Compliance department may either (1) report the breach immediately to HHS as described in subsection (b), or (2) maintain a log of such breaches and submit the log to HHS annually within 60 days of the end of the calendar year. Instructions for maintaining and submitting the log are posted on the HHS website. (45 CFR § 164.408(c))
    b. 500 or More Affected MEMBERS. If the breach involves 500 or more persons, the Compliance department shall notify HHS of the breach at the same time the

Compliance department notifies the MEMBER or next of kin. Instructions for maintaining and submitting the log are posted on the HHS website. (45 CFR § 164.408(b))

2. Notice to DHCS.
   a. CHPIV shall notify DHCS immediately upon the discovery of a suspected breach or security incident that involves Social Security Administration data. This notification will be provided by email upon discovery of the breach. If CHPIV is unable to provide notification by email, then CHPIV shall provide notice by telephone to DHCS.
   b. CHPIV shall notify DHCS within 24 hours by email (or by telephone if CHPIV is unable to email DHCS) of the discovery of:
      i. Unsecured PHI if the PHI is reasonably believed to have been accessed or acquired by an unauthorized person;
      ii. Any suspected security incident which risks unauthorized access to PHI and/or other confidential information;
      iii. Any intrusion or unauthorized access, use or disclosure of PHI in violation of the DHCS Contract; or
      iv. Potential loss of confidential data affecting the DHCS Contract.
   c. Notice shall be provided to CHPIV's DHCS Contract Manager. Further, CHPIV shall also notify the DHCS Privacy Office and the DHCS Information Security Office (collectively, "DHCS Contacts") using the DHCS Contact Information noted below.

DHCS Privacy Officer	DHCS Information Security Office
Privacy Office c/o: Office of HIPM Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov	Information Security Office DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov

   d. Notice shall be made using the current DHCS "Privacy Incident Reporting Form" ("PIR Form;" the initial notice of a security incident or breach that is submitted is referred to as an "Initial PIR Form") and shall include all information known at the time the incident is reported. The form is available online at https://www.dhcs.ca.gov/formsandpubs/laws/priv/Documents/Privacy-Incident-Report-PIR.pdf.
   e. DHCS requires CHPIV to immediately investigate a security incident or confidential breach. CHPIV must provide a complete report of the investigation to the DHCS contacts within ten (10) working days of the discovery of the security incident or breach. This "Final PIR Form" must include any applicable additional information not included in the Initial PIR Form. The Final PIR Form shall include an assessment of all known factors relevant to a determination of whether a breach occurred under the HIPAA PRIVACY RULES and other applicable federal and state laws. The report shall also include a full, detailed corrective action plan, including its implementation date and information on mitigation measures taken to halt and/or contain the improper use or disclosure. If DHCS requests

information in addition to that requested through a PIR Form, business associate shall make reasonable efforts to provide DHCS with such information. A "Supplemental PIR Form" may be used to submit revised or additional information after the Final PIR Form is submitted. DHCS will review and approve or disapprove CHPIV's determination of whether a breach occurred, whether the security incident or breach is reportable to the appropriate entities, if individual notifications are required, and CHPIV's corrective action plan. If CHPIV does not complete a Final PIR Form within the ten (10) working day timeframe, CHPIV must request approval from DHCS within the ten (10) working day timeframe of a new submission timeframe for the Final PIR Form.

f. Upon discovery of a breach or suspected security incident, intrusion, or unauthorized access, use or disclosure of PHI, CHPIV shall take:
   i. Prompt action to mitigate any risks or damages involved with the security incident or breach; and
   ii. Any action pertaining to such unauthorized disclosure required by applicable federal and state law.

I. Notice to Media. If a breach of PHI involves more than 500 residents in the state of California, CHPIV will also notify prominent media outlets in California. The notice shall be provided without unreasonable delay but no later than 60 days after discovery of the breach. The notice shall contain the same elements of information as required for the notice to the MEMBERS described above. The Senior Director of Compliance shall work with CHPIV senior leadership to develop an appropriate press release concerning the breach. (45 CFR § 164.406)

J. Notice from CHPIV Business Associate. If CHPIV's business associate discovers a breach of PHI, the business associate shall immediately notify the CHPIV Senior Director of Compliance of the breach. The business associate shall, to the extent possible, identify each person whose information was breached and provide such other information as needed by CHPIV to comply with this policy. Unless the Senior Director of Compliance directs otherwise and with the approval of the Senior Director of Compliance in writing such as via email, the business associate shall notify MEMBERS, HHS, DHCS, and, in appropriate cases, the media as described above after review and approval of any such notifications by CHPIV. (45 CFR § 164.410)

K. Delay of Notice Per Law Enforcement's Request. The Senior Director of Compliance shall delay notice to the MEMBER, HHS, DHCS, and the media if a law enforcement official states that the notice would impede a criminal investigation or threaten national security. If the officer's statement is in writing and specifies the time for which the delay is required, the Senior Director of Compliance shall delay the notice for the required time. If the officer's statement is verbal, the Senior Director of Compliance shall document the statement and the identity of the officer, and shall delay the notice for no more than 30 days from the date of the statement unless the officer provides a written statement confirming the need and time for delay. (45 CFR § 164.412)

L. Training Workforce Members. CHPIV shall train its workforce members concerning this Policy, including workforce members' obligation to immediately report suspected privacy violations. The Senior Director of Compliance shall ensure that this policy is included in training given to new workforce members, and thereafter in periodic training as relevant to the workforce members' job duties. (45 CFR § 164.530)

M. Sanctions. CHPIV workforce members may be sanctioned for a violation of this policy, including but not limited to the failure to timely report a suspected privacy violation. CHPIV may impose the sanctions it deems appropriate under the circumstances, including but not limited to termination of employment or contract. (45 CFR § 164.530)

N. Documentation. The Compliance department shall prepare and maintain documentation required by this Policy for a period of six (6) years or such other period of time as required by law or CHPIV's retention policy, including but not limited to reports or complaints of privacy violations; results of investigations, including facts and conclusions relating to the risk assessment; required notices; logs of privacy breaches to submit to HHS and DHCS; sanctions imposed; etc. (45 CFR § 164.530)

IV. DEFINITIONS

Whenever a word or term appears capitalized in this Policy and procedure, the reader should refer to the "Definitions" below.

TERM	DEFINITION
Department of Health Care Services (DHCS) Contract	The written agreement between CHPIV and the Department of Health Care Services (DHCS) pursuant to which CHPIV is obligated to arrange and pay for the provision of covered services to Members in the CHPIV Medi-Cal program, i.e., California's Medicaid health care program that pays for medical services for children and adults with limited income and resources and is supported by federal and state funding.
HIPAA Privacy Rules	Federal regulations promulgated under the Health Insurance Portability and Accountability Act provisions related to the privacy protection of Member PHI (45 CFR Part 160 and Part 164)
Member	A beneficiary enrolled in a CHPIV Medi-Cal program.
Protected Health Information (PHI)	Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Individually identifiable health information relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care. The information either identifies an individual or there is reasonable basis to believe the information can be used to identify the individual. (45 CFR § 160.103)

	Notice Of Privacy Practices	CMP-012
	Department	Compliance
	Functional Area	Compliance
	Impacted Delegate	☒ Subcontractor ☐ NA

DATES			
Policy Effective Date	10/9/2023	Reviewed/Revised Date	
Next Annual Review Due	10/9/2024	Regulator Approval	

APPROVALS			
Internal		**Regulator**	
Name	Elysse Tarabola	☐ DHCS ☐ DMHC	☒ NA
Title	Chief Compliance Officer		

ATTACHMENTS

- Attachment A – Member Notice of Privacy Practices

AUTHORITIES/REFERENCES

- CHPIV Contract with the Department of Health Care Services (DHCS) for Medi-Cal
- DHCS All Plan Letter (APL) 06-001: Notice of Privacy Practices and Notification of Breaches
- DHCS All Plan Letter (APL) 22-026: Interoperability and Patient Access Final Rule
- CHPIV Plan Compliance Plan
- Title 45, Code of Federal Regulations (C.F.R.), §160.202
- Title 45, Code of Federal Regulations (C.F.R.), §164.105(c)(2)
- Title 45, Code of Federal Regulations (C.F.R.), §164.508(a)(2)-(a)(4)
- Title 45, Code of Federal Regulations (C.F.R.), §164.508(b)(5)
- Title 45, Code of Federal Regulations (C.F.R.), §164.520(b)(1)(ii)(A) or (B)
- Title 45, Code of Federal Regulations (C.F.R.), §164.530(g)
- Patient Protection and Affordable Care Act §1557
- NCQA Standard MED5 Privacy and Confidentiality: Element A: Adopting Written Policies, Factor 1-2107

HISTORY

Revision Date	Description of Revision
10/9/2023	Policy creation

I. OVERVIEW

A. This NOTICE OF PRIVACY PRACTICES Policy (this Policy) identifies the required content of CHPIV's NOTICE OF PRIVACY PRACTICES (NPP) and the process by which the NPP is distributed to MEMBERS.

B. CHPIV ensures internal compliance with federal and state privacy and security requirements through ongoing monitoring.

C. CHPIV ensures its Business Associate's compliance with federal and state privacy and security requirements through ongoing monitoring and audits in accordance with this Policy and the BAA.

D. Violation of this Policy may result in disciplinary action, up to and including termination of employment and/or contract, civil and/or criminal action, and other legal and other remedies available to CHPIV.

II. POLICY

A. CHPIV MEMBERS have the right to adequate notice of the USES and DISCLOSURES of PROTECTED HEALTH INFORMATION (PHI) that may be made by CHPIV and of the MEMBERS' rights and CHPIV's legal duties with respect to PHI.

B. CHPIV shall provide information that directs MEMBERS on the process to file complaints with CHPIV and its regulators and will not retaliate against MEMBERS who file complaints when they believe their privacy rights have been violated.

C. CHPIV shall provide the NPP to MEMBERS and former MEMBERS as Required by Law, including providing the NPP upon enrollment and providing notice upon material revisions of the NPP in an easily accessible location on CHPIV's public website.

D. The CHPIV NPP shall describe steps the MEMBERmay consider taking to help protect privacy and security of their PHI.

E. Upon a material change to the NPP, CHPIV shall prominently post the change, or the revised NPP, on the CHPIV website by the effective date of the material change to the notice.

III. PROCEDURE

A. The content of the NPP shall be written in plain language and contain the following elements:

1. Mandated header;
2. Description and one (1) example each, of the types of USE and DISCLOSURES that CHPIV is permitted under state and federal regulations for the purposes of TREATMENT, PAYMENT, and HEALTH CARE OPERATIONS. If a USE or DISCLOSURE for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of Title 45, Code of Federal Regulations, Section 164.520 is prohibited or materially limited by other applicable law, the description of such USE or DISCLOSURE must reflect the more stringent law;
3. A description of the types of USES and DISCLOSURES that require an authorization under Section 164.508(a)(2)-(a)(4), a statement that other USE and DISCLOSURES not described in this notice will be made only with the Member's written authorization, and

a statement that the MEMBER may revoke such authorization as provided by Section 164.508(b)(5);

4. Statement to describe the Member's rights concerning his or her PHI, how to exercise these rights, and restrictions on such rights, which shall include information on:
    a. Restrictions concerning certain USE and DISCLOSURES of PHI, and provision that CHPIV is not required to agree to those restrictions, except in case of a DISCLOSURE restricted under Section 164.522(a)(1)(vi);
    b. Right to receive confidential communications of PHI;
    c. Right to inspect and copy PHI;
    d. Right to request amendment to PHI;
    e. Right to receive accounting of DISCLOSURES, with certain exceptions; and
    f. Right to receive a paper copy of the NPP, in accordance with this Policy.
5. Statement specifically describing CHPIV's duties and rights under the privacy rule, including:
    a. A statement that CHPIV is Required by Law to maintain the privacy of the Member's PHI, to provide individuals with notice of its legal duties and privacy practices with respect to PHI, and to notify affected MEMBERS following a breach of unsecured PHI, and in accordance with CHPIV policies, which shall include processes to ensure internal protection of verbal (i.e., when talking to individuals on the telephone or in person about a Member), and written information;
    b. The responsibility to abide by the terms of the NPP currently in effect;
    c. Reserve CHPIV's right to make changes to the terms of the NPP when we make changes to our privacy practices; and
    d. A description of how CHPIV provides MEMBERS with a revised NPP.
6. Statement that the MEMBER may file a complaint as part of their privacy rights, and without retaliation, to CHPIV's Customer Service Department or Privacy Officer, the California Department of Health Care Services (DHCS), and/or the United States Department of Health and Human Services (HHS), if the MEMBER believes his or her privacy rights have been violated, and include contact title and telephone number for filing the complaint with CHPIV, or to get further information concerning the notice. The contact information should include:
    a. Attn: Privacy Officer
       CHPIV
       512 west Aten Rd
       Imperial, CA
       Telephone: 760-332-6447
    b. CHPIV Customer Service Department
       Toll-free: 1-833-236-4141
       TTY: 711
    c. California Department of Health Care Services
       Privacy Officer

c/o: Office of HIPAA Compliance
Department of Health Care Services
P.O. Box 997413 MS 4722
Sacramento CA 95899-7413
Email: privacyofficer@dhcs.ca.gov
Telephone: 1-916-445-4646
Fax: 1-916-440-7680

d. U.S. Dept. of Health and Human Services
Office for Civil Rights
Regional Manager
90 7th Street Suite 4-100
San Francisco CA 94103
Phone: 1-800-368-1019
Fax: 1-415-437-8329
TDD: 1-800-537-7697
Email: OCRComplaint@hhs.gov

7. Effective date of the notice.
   a. The NPP shall be made available to anyone, upon request, by calling or writing to the CHPIV Customer Service Department. CHPIV's Customer Service Department shall make the NPP available in THRESHOLD LANGUAGES to anyone by mail, in person, or through the CHPIV website. CHPIV shall distribute the NPP by:
      i. Ensuring initial distribution by mail to all MEMBERS;
      ii. Including copies in all new enrollment packets;
      iii. Posting a copy in the Customer Service Department lobby in THRESHOLD LANGUAGES;
      iv. Posting the NPP on the CHPIV website;
      v. Providing a revised NPP, or information about the material change and how to obtain the revised NPP, in the next annual mailing to MEMBERS;
      vi. Notifying all MEMBERS at least once every three (3) years that a copy of the NPP is available upon request or may be obtained on the CHPIV website at www.CHPIV.org; and
      vii. Ensuring all mailings of the NPP comply with CHPIV's Cultural and Linguistic Services guidelines.

B. Documentation and Retention:
1. CHPIV shall document compliance with this Policy and retain copies of the notices issued for a period of ten (10) years from the effective date of the notice.

IV. DEFINITIONS

Whenever a word or term appears capitalized in this Policy and procedure, the reader should refer to the "Definitions" below.

TERM	DEFINITION
Disclosure/Disclose	The release, transfer, provision of access to, or divulging in any manner of information outside of the entity holding the information. (45 CFR § 160.103)
Health Care Operations	Includes without limitation in accordance with federal regulation, quality assessment and improvement activities, care management, professional review, compliance and audits, health insurance underwriting, premium rating and other activities related to a contract and health benefits, management and administration activities, customer services, resolution of internal grievances, business planning, and development and activities related to compliance with the privacy rule. (45 CFR § 164.501)
Member	A beneficiary enrolled in a CHPIV Medi-Cal program.
Notice of Privacy Practices (NPP)	Notice provided to a Member that describes CHPIV's practices in the Use and Disclosure of Protected Health Information, Member rights, and CHPIV legal duties with respect to Protected Health Information.
Payment	Includes without limitation in accordance with federal regulation: 1. Determination of eligibility, risk adjustments based on Member health status and demographics, billing claims management, and collection activities; 2. Review of health care services regarding medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and 3. Utilization review activities including pre-certification, preauthorization, concurrent, or retrospective review of services. (45 CFR § 164.501)
Protected Health Information (PHI)	Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Individually identifiable health information relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care. The information either identifies an individual or there is reasonable basis to believe the information can be used to identify the individual. (45 CFR § 160.103)
Threshold Languages	Those languages identified based upon State requirements and/or findings of the Population Needs Assessment (PNA).

TERM	DEFINITION
Treatment	The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. (45 CFR § 164.501)
Use	With respect to individually identifiable health information, means the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. (45 CFR § 160.103)

Notice of Privacy Practices
Effective September 1, 2023

CHPIV offers you access to health care through the Medi-Cal program. We are required by state and federal law to protect your health information. After you become eligible and enroll in our health plan, Medi-Cal sends your information to us. We also get medical information from your doctors, clinics, labs and hospitals to approve and pay for your health care.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

YOUR RIGHTS
When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

Get a copy of your health and claims records	• You can ask to see or get a copy of your health and claims records and other health information we have about you. You must make this request in writing. You will be sent a form to fill out and we may charge a fair fee for the costs of copying and mailing records. • You must provide a valid form of ID to view or get a copy of your health records. • We will provide a copy or a summary of your health and claims records, usually within 30 days of your request. • We may keep you from seeing certain parts of your records for reasons allowed by law. • CHPIV does not have complete copies of your medical records. If you want to look at, get a copy of, or change your medical records, please contact your doctor or clinic.
Ask us to correct health and claims records	• You have the right to send a written request to ask that information in your records be changed if it is not correct or complete. You must make your request in writing. • We may refuse your request if the information is not created or kept by CHPIV, or we believe it is correct and complete, but we will tell you why in writing within 60 days. • If we don't make the changes you ask, you may ask that we review our decision. You may also send a statement saying why you disagree with our records, and your statement will be kept with your records.
Request confidential communications	• You can ask us to contact you by your preferred method of contact (for example, home or work phone) or to send mail to a different address.

	• We will consider all fair requests. We must say "yes" if you tell us you would be in danger if we do not.
Ask us to limit what we use or share	• You can ask us not to use or share certain health information for treatment,payment, or our operations. • We are not required to agree to your request, and we may say "no" if it would affect your care.
Get a list of those with whom we've shared information	• You can ask for a list (accounting) of the times we've shared your health information for six years prior to the date you ask, who we shared it with, and why. • We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We'll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within12 months.
Get a copy of this privacy notice	• You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.
Choose someone to act for you	• If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information. • We will make sure the person has this authority and can act for you before we take any action.
Use a self-pay restriction	• If you pay the whole bill for a service, you can ask your doctor not to share the information about that service with us. If you or your provider submits a claim to CHPIV, we do not have to agree to a restriction. If a law requires the disclosure, CHPIV does not have to agree to your restriction.
File a complaint if you feel your rights are violated	• If you feel we have violated your rights, you can complain by contacting us using the information in this notice. • We will not retaliate against you for filing a complaint.

Your Choices: For certain health information, you can tell us your choices about what we share. If you have a preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions. In most cases, if we use or share your Protected Health Information (PHI) outside of treatment, payment

or operations, we must get your written permission first. If you give us your permission, you may take it back in writing at any time. We can't take back what we used or shared when we had your written permission, but we will stop using or sharing your PHI in the future.

In these cases, you have both the right and choice to tell us to:	• Share information with your family, close friends, or others involved in payment for your care. • Share information in a disaster relief situation. • Contact you for fundraising efforts. *If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.*
In these cases we never share your information unless you give us written permission:	• Psychotherapy Notes: We must obtain your authorization for any use or disclosure of psychotherapy notes, except to carry out certain treatment, payment or health care operations. • Marketing purposes, unless allowed by law or regulation. • Sale of your information.

Our Uses and Disclosures: Your information may be used or shared by CHPIV only for treatment, payment and health care operations related with the Medi-Cal program in which you are enrolled. We may use and share your information in health information exchanges with providers involved in the care you receive. The information we use and share includes, but is not limited to:

- Your name
- Address
- History of care and treatment given to you
- Cost or payment for care

Help manage the health care treatment you receive	• We can use your health information and share it with professionals who are treating you.	***Example:*** *A doctor sends us information about your diagnosis and treatment plan so we can arrange additional services. We will share information with doctors, hospitals and others in order to get you the care you need.*

Run our organization (health care operations)	• We can use and share your information to run our organization and contact you when necessary. • **We are not allowed to use genetic information to decide whether we will give you coverage and the price of that coverage.**	**Example:** *We use health information about you to develop better services for you, which may include reviewing the quality of care and services you receive. We may also use this information in audits and fraud investigations.*
Pay for your health services	• We can use and share your health information as we pay for your health services.	***Example:*** *We share information with the doctors, clinics and others who bill us for your care. We may also forward bills to other health plans or organizations for payment.*
Administer your plan	We may share your health information with the Department of Health Care Services (DHCS) or the Centers for Medicare & Medicaid Services (CMS) for plan administration.	***Example:*** *DHCS contracts with us to provide a health plan, and we provide DHCS with certain statistics.*

How else can we use or share your health information? We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes. For more information see: **www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.**

Help with public health and safety issues	We can share health information about you for certain situations such as: • Preventing disease • Helping with product recalls • Reporting adverse reactions to medicines • Reporting suspected abuse, neglect or domestic violence • Preventing or reducing a serious threat to anyone's health or safety

Comply with the law	• We will share information about you if state or federal laws require it, including with the U.S. Department of Health and Human Services if it wants to see that we are complying with federal privacy law.
Respond to organ and tissue donation requests and work with a medical examiner or funeral director	• We can share health information about you with organ procurement organizations. • We can share health information with a coroner, medical examiner or funeral director when an individual dies.
Address workers' compensation, law enforcement and other government requests	We can use or share health information about you: • For workers' compensation claims • For law enforcement purposes or with a law enforcement official • With health oversight agencies for activities authorized by law • For special government functions, such as military, national security and presidential protective services.
Respond to lawsuits and legal actions	• We can share health information about you in response to a court or administrative order, or in response to a subpoena.
Comply with special laws	• There are special laws that protect some types of health information, such as mental health services, treatment for substance use disorders, and HIV/AIDS testing and treatment. We will obey these laws when they are stricter than this notice. • There are also laws that limit our use and disclosure for reasons directly connected to the administration of CHPIV's programs.

OUR RESPONSIBILITIES

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.
- For more information see: https://www.hhs.gov/hipaa/index.html.

Changes to the Terms of This Notice

CHPIV can change the terms of this notice, and the changes will apply to all information we have about you. If that happens, we will update the notice and notify you. We will also post the updated notice on our website.

How to Contact Us to Use Your Rights

If you want to use any of the privacy rights explained in this notice, please write us at:
Privacy Officer
Attn: CHPIV
512 west Aten Rd
Imperial, CA
Telephone: 760-332-6447
Or call CHPIV's Customer Service department at: **1-833-236-4141**
TTY: **711**

If you believe that we have not protected your privacy and wish to file a complaint or grievance, you may write or call CHPIV at the address and phone number above. You may also contact the agencies below:

California Department of Health Care Services
Privacy Officer
C/O: Office of HIPAA Compliance
Department of Health Care Services
P.O. Box 997413, MS 4722
Sacramento, CA 95899-7413
Email: privacyofficer@dhcs.ca.gov
Phone: 1-916-445-4646
Fax: 1-916-440-7680

U.S. Dept. of Health and Human Services
Office for Civil Rights
Regional Manager
90 Seventh St., Suite 4-100
San Francisco, CA 94103
Email: OCRComplaint@hhs.gov
Phone: 1-800-368-1019
Fax: 1-415-437-8329
TDD: 1-800-537-7697

Use Your Rights Without Fear

CHPIV cannot take away your health care benefits nor do anything to hurt you in any way if you choose to file a complaint or use any of the privacy rights in this notice. This notice applies to CHPIV's Medi-Cal health care program.

CHPIV's Medi-Cal program contracts with DHCS to provide benefits under the Medi-Cal program to its members. CHPIV complies with applicable federal civil rights laws and does not

discriminate on the basis of race, color, national origin, age, disability, or sex. Please call our Customer Service number at 1-833-236-4141, 24 hours a day, 7 days a week. TDD/TTY users can call 711.

English: ATTENTION: If you speak a language other than English, language assistance services, free of charge, are available to you. Call 1-833-236-4141 (TTY: 711).

Spanish: ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-833-236-4141 (TTY: 711).

Vietnamese: CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 1-833-236-4141 (TTY: 711).

Chinese: 注意：如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 1-833-236-4141 (TTY: 711).

Korean: 주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. 1-833-236-4141 (TTY: 711)

Farsi: توجه :اگر به زبان فارسی گفتگو می کنید، تسهيلات زبانی بصورت رایگان برای شما فراهم می باشد. 1-833-236-4141 (TTY: 711) تماس بگیرید.

Arabic: ملحوظة :إذا كنت تتحدث بلغة أخري غير الإنجليزية، فإن خدمات المساعدة اللغوية تتوفر لك بالمجان .اتصل علي الرق م1- 833-236-4141 (TTY: 711)

QUIZ

1. The primary Federal Law pertaining to the medical information privacy is:
    a. American Recovery and Reinvestment Act (ARRA)
    b. Health Information Technology for Economic and Clinical Health Act (HITECH)
    c. Health Insurance Portability and Accountability Act (HIPAA)
    d. All of the above
    e. None of the above
2. What is PHI?
    a. Privacy Health Information
    b. Protected Health Information
    c. Patient Health Insurance
3. Which of the following are examples of PHI?
    a. Patient's Name
    b. Patient's Date of Birth
    c. Patient's Address
    d. Medical Record Number
    e. Admission date, time, and reason
    f. All of the above
    g. None of the above
4. The "minimum necessary" requirement of HIPAA refers to using or disclosing/releasing only the minimum PHI necessary to accomplish the purpose for which it is being used, requested, or disclosed.
    a. True
    b. False
5. The HIPAA Privacy Rule protects all PHI, electronic, verbal and written.
    a. True
    b. False
6. If you need to report a HIPAA concern or violation, which of the following can you do?
    a. Contact my organization's HIPAA Compliance Officer
    b. Contact my supervisor or manager
    c. All of the above

   d. None of the above
7. HIPAA mandates that members have the right to:
   a. Request restrictions on release of PHI
   b. File complaints
   c. Receive the notice of privacy practices
   d. Access medical records
   e. All of the above
   f. None of the above
8. It is not mandatory to secure emails for HIPAA protected information on outgoing email
   a. True
   b. False
9. Only access the information your job requires for treatment, payment, Healthcare Operations
   a. True
   b. False
10. An authorization form is not needed prior to releasing PHI
   a. True
   b. False

General Compliance Training

Training Material

Quiz Submission Due: December 11, 2023

Table of Contents

I. Objectives 3

II. Why Do I Need Training? 3

III. What is an Effective Compliance Program? 3

IV. Compliance Program Requirements 3

A. Requirements of an Effective Compliance Program 3

B. Conduct 3

C. Oversight 4

D. Training and Education 4

E. Communication 5

F. Discipline 5

G. Monitoring 5

H. Reporting 5

V. Ethics: Do the Right Thing 6

VI. What is Expected of Me? 6

VII. What is Non-Compliance? 6

VIII. Examples of Non-Compliance 6

IX. Non-Compliance Affects All 8

X. How to Report Non-Compliance 8

XI. Reporting Non-Compliance 8

XII. After Non-Compliance is Detected 9

XIII. Internal Monitoring and Audits 9

XIV. Compliance is Everyone's Job 9

XV. Appendix 10

XVI. Disclaimer 10

XVII. APPENDIX 10

I. Objectives

A. After this course you should correctly

1. Recognize the 7 elements of an effective Compliance Program
2. Understand Ethics-Doing the right thing
3. Recognize how compliance program violations should be reported

II. Why do I Need Training?

A. Compliance is Everyone's Responsibility

B. *Failure to follow Medicare, CMS guidance, Health Plan and regulatory agency requirements can lead to serious consequences, including:

1. Contract termination
2. Criminal penalties for both the organization and the offending individual
3. Exclusions from participating in all Federal health care programs
4. Civil monetary penalties for both the organization and the offending individual

III. What is an Effective Compliance Program?

A. An effective compliance program fosters a culture of compliance within an organization, and:

1. Prevents, detects and corrects non-compliance
2. Is tailored and implemented to an organization's unique operations and circumstances
3. Has adequate resources
4. Promotes the Code of Conduct
5. Establishes clear lines of communication

IV. Compliance Program Requirements

A. Requirements of an Effective Compliance Program:

1. Written Policies, Procedures and Standards of Conduct
2. Compliance Officer, Compliance Committee and High-Level Oversight
3. Effective Training and Education
4. Effective Lines of Communication
5. Well-Publicized Disciplinary Standards
6. Effective System for Routine Monitoring, Auditing and Identifying Compliance Risks
7. Procedures and System for Prompt Response to Compliance Issues
8. 42 C.F.R. §§422.503(b)(4)(vi)

B. Conduct

1. Written Policies, Procedures and Standards of Conduct
    a. Policies articulate commitment to comply with all applicable Federal and State standards and describe compliance expectations according to the Code of Conduct.
2. CHPIV has distributed policies and the Standard of Conduct via email and requested an attestation form in return
    a. Code of Conduct: Standards
        i. *Excerpt*: Standard 1. CHPIV Culture, Workplace Environment and Brand
            a. ***Non-Retaliation/Intimidation:*** CHPIV has a zero-tolerance policy for intimidation and retaliation. CHPIV encourages and supports team members in reporting potential/confirmed violations of this Code of Conduct and potential/confirmed non-compliance with CHPIV policies or applicable law
    b. 42 C.F.R. §§422.503(b)(4)(vi)

C. Oversight
1. Designated Compliance Officer, Compliance Committee
    a. Senior Director of Compliance: Chelsea Hardy
    b. Community Health Plan of Imperial Valley designated a Compliance Officer and a compliance committee accountable and responsible for the activities and status of the compliance program, including issues identified, investigated and resolved by the compliance program. The senior management and governing body are engaged and exercise reasonable oversight of the compliance program.

D. Training and Education
1. Effective Compliance Education and Training
    a. This covers the elements of the compliance plan as well as preventing, detecting and reporting FWA.
    b. Training and education is covered in many ways. The training and education are to be tailored for the different employees and their roles and responsibilities. This is attained through Annual Compliance Training, staff meetings, email notifications and departmental educational trainings.
    c. Per CMS, Refer to Chapter 21, GC training 50.3.1 for a review of laws that govern employee conduct in the

Medicare program (https://www.cms.gov/regulations-and-guidance/guidance/manuals/downloads/mc86c21.pdf)

E. Communication
    1. Effective Lines of Communication
        a. Chain of Command
        b. Management Team
        c. Compliance Department
        d. Hot Line-Anonymous Reporting

F. Discipline
    1. Community Health Plan of Imperial Valley must enforce standards through well-publicized disciplinary guidelines. These should be provided during new employee orientation, Annual Compliance training, staff meetings and be present in policy to articulate expectation for reporting compliance issues and assist in their resolution when appropriate. To outline actions such as:
        a. Mandatory training or re-training
        b. Disciplinary action that is consistent and equitable
        c. Termination

G. Monitoring
    1. Effective System for Routine Monitoring and Identification of Compliance Risk
        a. The system should include routine internal monitoring and audits of operations to evaluate compliance with requirements. As appropriate, external audits, to evaluate the sponsor's, including FDRs', compliance with CMS requirements and the overall effectiveness of the compliance program.
            i. Audit compliance with regulations, contractual agreements and all State and Federal laws
            ii. Monitor activities are performed as expected and ensure corrective actions are undertaken and effective

H. Reporting
    1. Established System to Promptly Respond to Compliance Issues
        a. Establish and implement procedures and a system for promptly responding to compliance issues as they are raised, investigating potential compliance problems as identified during self-evaluations and audits, correcting such problems promptly and thoroughly to reduce the potential for recurrence, and ensuring ongoing compliance

with CMS, state regulatory agencies and Health Plan requirements.

V. Ethics: Do the Right Thing

A. It is really that simply… Do the right thing by:
   1. Conducting yourself in an ethical and legal manner
   2. Acting fairly and honestly
   3. Adhering to high ethical standards in all you do
   4. Acting with integrity, transparency and accountability
   5. Complying with all laws, regulations and regulatory agencies
   6. Reporting suspected/actual violations

VI. What is Expected of me?

A. Follow company Code of Conduct
B. Read and understand company policies
C. Know how to report violations or suspected non-compliance
   1. Compliance Policy
      a. *Excerpt: Escalation of Non-Compliance Issue (*CMP-007)
         i. ***Reporting Noncompliance***: Any individual who becomes aware of a noncompliance issue must report it immediately to their immediate supervisor, any member of the leadership team, Chief Compliance Officer, or Compliance department. Anonymous reporting is available through the CHPIV website and Compliance Hotline.

VII. What is Non-Compliance?

A. Non-compliance is any conduct that does not conform with State and Federal law and/or program requirements, with contract requirements, or with ethical and business policies. Areas of risk include (but are not limited to):
   1. Agent/Broker misrepresentation
   2. Appeals and grievance review (for example, coverage and organization determinations)
   3. Member notices
   4. Conflicts of interest
   5. Claims processing
   6. Credentialing and provider networks
   7. Documentation and Timeliness requirements
   8. Health Insurance Portability and Accountability Act (HIPAA)
   9. Marketing and enrollment
   10. Pharmacy, formulary, and benefit administration
   11. Quality of care

VIII. Examples of Non-Compliance

A. Scenario 1
    1. My co-worker changed a date on a member's authorization request to avoid getting in trouble. She is my friend and she said she will not do it again, so I won't say anything.
    2. Explanation: Covering up unethical behavior is wrong. While you don't want your friend to be in trouble, you are harming the member and breaking the company code of conduct.
B. Scenario 2
    1. My friend's neighbor is ill and came in to see the doctor I work for. My friend called me on behalf of the neighbor's spouse wanting information on the visit. My friend says the neighbor's spouse only wants to confirm that neighbor wasn't lying about the visit.
    2. Explanation: Releasing patient information without the proper reason/authorization is prohibited. Even though you may desire to help your friend and the neighbor's spouse, providing any information on the visit is non-compliance unless the neighbor authorized their spouse right of access.
C. Scenario 3
    1. You receive an alert about claims from XYZ Lab. For the last six months, the lab consistently billed for code 80055 (CPT Code for a prenatal panel with CBC). In your review, you find that the code is used for both male and female patients and that reimbursement for code 80055 is higher than the standard codes for a CBC. You also find that orders are from Dr. John Doe, your favorite doctor.
    2. Explanation: This is considered a form of upcoding, which is fraud. Irrespective that Dr. Doe is your favorite doctor, your findings should be reported immediately so that the matter may be investigated. Failure to report is considered non-compliance and, if fraud is proven, there is a risk of being considered complicit with the fraud.
D. Scenario 4
    1. A parent brings their child to an appointment at your office. As you check-in the child, the child's demographic states that the child's DOB would make the child 8 years old, but the child in your office appears to be significantly younger. This is the last patient, you don't want any trouble, and you just want to go home.
    2. Explanation: The parent is committing fraud and by covering up for a patient – whether intentionally or otherwise – you are in

violation of your provider's office patient verification policy, and are at risk of being considered complicit in the fraud as well as excluded from participation in most healthcare programs.

IX. Non-Compliance Affects All

A. Without programs to prevent, detect and correct non-compliance, we all risk:
    1. Potential and possibly catastrophic harm to members through:
        a. Delayed services
        b. Denial of benefits
        c. Difficulty in using provider of choice
        d. Other hurdles of care
    2. Failure to follow the requirements can lead to serious consequences, such as:
        a. Financial sanctions
        b. Contract termination
        c. Criminal penalties
        d. Exclusions from participating in most health care programs

X. How to Report Potential Non-Compliance

A. Employees of CHPIV
    1. Speak to your manager
    2. Call Compliance Department
    3. Access Compliance@chpiv.org or call Compliance Hotline at 800-919-4947 to anonymously report
B. Members and Providers can:
    1. Access Compliance@chpiv.org or call Compliance Hotline at 800-919-4947
    2. Call 1-800-MEDICARE
C. Do Not Hesitate to Report Non-Compliance When you report suspected non-compliance in good faith, CHPIV cannot retaliate against you
    1. Code of Conduct: Standards
        a. *Excerpt*: Standard 1. CHPIV Culture, Workplace Environment and Brand
            i. ***Non-Retaliation/Intimidation:*** CHPIV has a zero-tolerance policy for intimidation and retaliation. CHPIV encourages and supports team members in reporting potential/confirmed violations of this Code of Conduct and potential/confirmed non-compliance with CHPIV policies or applicable law

XI. Reporting Non-Compliance

A. Who is a "Whistleblower"? A Whistleblower is any individual who exposes information or activity that may be deemed illegal, dishonest, or violates professional or clinical standards.
B. When reporting in “good faith,” an employer cannot retaliate against you for exercising your rights under the Department of Labor’s “Whistleblower Protection” laws.
C. Scenario
    1. “After I reported irregularities in my department, my manager began excluding me from meetings and moved me to another department.”
    2. Explanation: Retaliation or intimidation is not tolerated. The manager’s behavior is unacceptable and should be reported to leadership or to Compliance.

XII. After Non-Compliance is Detected

A. Non-compliance must be investigated immediately and corrected promptly
    1. Internal monitoring and auditing should ensure:
        a. No recurrence of the same non-compliance
        b. Ongoing regulatory compliance requirements
        c. Efficient and effective internal controls
        d. Enrollees are protected

XIII. Internal Monitoring and Audits

A. Monitoring and auditing to test and confirm compliance with policies, laws, contracts, State and Federal regulations is part of ensuring an effective compliance program
    1. Internal Monitoring activities include regular reviews confirming ongoing compliance and taking effective corrective actions.
    2. Internal Auditing is a formal review of compliance with a particular set of standards (policies, laws, regulations, contract commitments) used as base of measures.
    3. Medicare Managed Care Manual
    4. Chapter 21 – Compliance Program Guidelines and Prescription Drug Benefit Manual
    5. Chapter 9 - Compliance Program Guidelines
    6. Section 50.6.1 – Routine Monitoring and Auditing

XIV. Compliance is Everyone’s Job

A. Prevent
    1. Operate within ethical expectations to prevent non-compliance
B. Detect & Report
    1. If you see it, report it - report potential non-compliance
C. Correct

1. Correct non-compliance that includes ongoing monitoring to protect members

XV. Appendix

A. Appendix: Laws and Regulations to Consider in Standards of Conduct and/or Training (Chapter 21-Rev. 109 & Chapter 9-Rev. 15-Issued: 07-27-12, Effective: 07-20-12; Implementation 07-20-12)
    1. Title XVIII of the Social Security Act
    2. Medicare regulations governing Parts C and D found at 42 CFR§§ 422 and 423 respectively
    3. Patient Protection and Affordable Care Act (Pub. 1., No. 111-148, 124 Stat. 119)
    4. Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191)
    5. False Claims Acts (31 U.S.C. §§ 3729-3733)
    6. Federal Criminal False Claims Statutes (18 U.S.C. §§ 287, 1001)
    7. Anti-Kickback Statute (42 U.S.C. § 1320a-7b(b))
    8. The Beneficiary Inducement Statute (42 U.S.C §1320a-7a(a)(5))
    9. Civil monetary penalties of the Social Security Act (42 U.S.C. § 1395w-27 (g))
    10. Physician Self-Referral ("Stark") Statute (42 U.S.C § 1395nn)
    11. Fraud and Abuse, Privacy and Security Provisions of the Health Insurance Portability and Accountability Act, as modified by HITECH Act
    12. Prohibitions against employing or contracting with persons or entities that have been excluded from doing business with the Federal Government (42 U.S.C. §1395w-27(g)(1)(G)
    13. Fraud Enforcement and Recovery Act of 2009
    14. Department of Labor Whistleblower Protection Laws

XVI. Disclaimer

A. This course was prepared as a service and is not intended to grant rights or impose obligations. This course may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. Readers are encouraged to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

XVII. APPENDIX

A. Code of Conduct
    1. Standards
        a. Standard 1. CHPIV Culture, Workplace Environment and Brand

B. Escalation of Non-Compliance Issue (CMP-007)

Code of Conduct

Compliance & Policy Committee Approval on: 08/10/23
Commission Approval on: 08/14/2023

Community Health Plan
OF IMPERIAL VALLEY

Table of Contents

I. Introduction 3
II. Standards 4
Standard 1. CHPIV Culture, Workplace Environment and Brand 4
Standard 2. Compliance with the Law 5
Standard 3. Regulatory Entities and Government Inquiries 6
Standard 4. Business Relationships and Conflicts of Interest Avoidance 6
Standard 5. Public Entity Integrity 7
Standard 6. Record Keeping and Confidentiality 7
III. Addressing Noncompliance with the Code of Conduct 8
IV. Resources 8

I. Introduction

Local Health Authority for Imperial County (hereafter, "Community Health Plan of Imperial Valley" or "CHPIV") maintains this Code of Conduct as framework for operating in accordance with applicable regulations and laws, organization policies and procedures, and our guiding principles. CHPIV is committed to ensuring compliance with all pertinent federal and state requirements. The Code of Conduct serves as a resource to guide you in fulfilling your business responsibilities ethically. CHPIV developed this Code of Conduct based on the principles reflected in our Mission, Vision, and Values:

> **Mission** The mission of the Community Health Plan of Imperial Valley is to work with community residents and stakeholders in both the public and private sectors to: (1) advance opportunities for improved health and access to comprehensive health care services; (2) promote the long-term viability of safety net providers; (3) increase prevention, education, and early intervention services; and (4) partner with Medi-Cal managed care plans to monitor and improve the local healthcare system.
>
> **Vision** Healthy Community, Healthy Residents
>
> **Values** INTEGRITY. Honestly, Trustworthiness, hardworking, accountability for our actions, and helpful to all. RESPECT. Treating people how you would like to be treated. RESPONSIBILITY: Own the service we provide. TEAMWORK: Supporting your colleagues and team members when they need you and vice versa, them being there when you need them. SERVANT MANAGEMENT. Serve the interests of all.

The Code of Conduct applies to the CHPIV Commission (governing board) and all applicable committees that report to the Commission, CHPIV employees, affiliates, officers, community advisory committees, management, temporary staff, volunteers, contractors, consultants, vendors, interns, and providers (hereinafter collectively referred to as "Applicable Individuals").

Applicable Individuals are not only encouraged but are obligated to act with integrity and honesty in every aspect of their work. This commitment goes beyond merely following rules; it's about fostering a culture of transparency and respect, ensuring we always act in the best interests of those we serve and represent. Applicable Individuals hold a shared responsibility in guaranteeing compliance and plays a crucial role in upholding our Code of Conduct. If at any point you believe that our standards may be compromised, it is not only your right but your responsibility to raise such concerns. Applicable Individuals are required to:

- Submit an annual acknowledgement confirming you have read and understand the Code of Conduct.

- Participate in any required Code of Conduct training.
- Understand and comply with regulations, applicable laws, and CHPIV policies.
- Disclose any potential or actual conflicts of interest.
- Report possible or confirmed Code of Conduct violation to your immediate supervisor, the Chief Compliance Officer, or via the Compliance Hotline at 800-919-4947.

II. Standards

Standard 1. CHPIV Culture, Workplace Environment and Brand

- **Member-centric:** CHPIV operates in service of its members with the mission to provide equitable, high-quality care in Imperial County. CHPIV places its members at the center of its decisions and operations.
- **Respect for Others:** CHPIV team members and Applicable Individuals must treat one another with respect and professionalism. Each team member is a valued and integral part of creating a healthy, successful workplace environment and of driving equitable, high-quality care for CHPIV members.
- **Nondiscrimination:** CHPIV does not tolerate discrimination based on race, color, religion, gender, national origin, ancestry, age, physical disability, mental disability, medical condition, family care leave status, veteran status, marital status, sexual orientation, or any other category protected under applicable laws.
- **Non-harassment:** CHPIV does not tolerate harassment, bullying, violence, or threats of violence of any kind.
- **The CHPIV Brand (branding & media requests):** If the media contacts you to discuss CHPIV, rather than speaking with them directly, please direct them to Larry Lewis (LLewis@chpiv.org) and Michelle Ortiz (MOrtiz@chpiv.org).
- **Use of CHPIV Systems:** CHPIV computers, networks, and mobile communication devices should be used for work purposes only. The following activities are prohibited. This list is not exhaustive and other activities will be addressed on a case-by-case basis.
    - Sharing login credentials
    - Distribution of inappropriate materials
    - Excessive use of email accounts for personal purposes
    - Excessive access to websites that are not work-related
    - Unsecure transmittal of sensitive information, PII, and PHI
    - Use of non-CHPIV e-mail services to send or receive PII, PHI, or other sensitive company information
    - Removal of CHPIV data

- Disabling or bypassing security controls
- Installing software
- Attempts to access unauthorized systems, networks, or data
- Failure to report lost or stolen computers/communication devices

- **Non-Retaliation/Intimidation:** CHPIV has a zero-tolerance policy for intimidation and retaliation. CHPIV encourages and supports team members in reporting potential/confirmed violations of this Code of Conduct and potential/confirmed non-compliance with CHPIV policies or applicable law.

Standard 2. Compliance with the Law

- **Fraud, Waste, and Abuse:** CHPIV maintains a Fraud, Waste and Abuse Program which describes examples of potential fraud, waste, and abuse, CHPIV and subcontractor obligations, and potential sanctions/disciplinary action related to violations. CHPIV and Applicable Individuals are prohibited from engaging in conduct that violates Fraud, Waste, and Abuse laws. CHPIV requires its staff, Commission members, and subcontractors/FDRs to complete required training regarding Fraud, Waste, and Abuse. CHPIV is committed to the prevention, detection, and reporting of Fraud, Waste and Abuse. All individuals are responsible for reporting suspected Fraud, Waste, and Abuse to Compliance@chpiv.org.
- **Anti-Trust:** CHPIV and Applicable Individuals are required to comply with applicable anti-trust laws. Individuals who encounter business decisions with potential for anti-trust law implications are required to seek advice from legal counsel.
- **Political Activities:** CHPIV funds, property, and resources cannot be used for any political activity. CHPIV and applicable individuals may not imply that their personal political views represent CHPIV.
- **Protecting Confidential Member Information:** CHPIV safeguards all member confidential information, including but not limited to protected health information (PHI) and personally identifiable information (PII), in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), the California Security Breach Notification Law, the California Confidentiality of Medical Information Act (CCMIA), and other applicable laws. CHPIV maintains policies and procedures that govern how the organization and Applicable Individuals are to ensure member confidentiality rights.
- **Protecting Proprietary Information:** In accordance with the Public Records Act, CHPIV safeguards confidential proprietary information, including contractor information, provider identification numbers, Medi-Cal license information, Medicare numbers, social security numbers, and other identifying information.

- **Use of Proprietary Information:** Applicable Individuals may not use proprietary CHPIV information for their own personal benefit, during and after employment with CHPIV.
- **Compliance Training:** CHPIV requires its employees, interns, volunteers, and Commission to complete Compliance Training within 90 days of hire and annually. Compliance training includes topics related to Fraud, Waste, and Abuse, HIPAA, CHPIV's Compliance Program, and obligations to report potentially non-compliant activities.

Standard 3. Regulatory Entities and Government Inquiries

- **Communicating with Regulators/Government Entities:** CHPIV is committed to maintaining open, accurate, and truthful communications with regulators and applicable government entities. Communications with regulators are managed and coordinated through the Compliance department in collaboration with CHPIV leadership. If a regulatory or government entity contacts you, please reach out to the Compliance department (Compliance@chpiv.org) for guidance on how to proceed.
- **Exclusion from Government Programs/Participation Status:** CHPIV does not hire or conduct business with any Applicable Individuals who are excluded from participation in any federal or state health care program. Applicable Individuals are required to disclose if they are or become ineligible, whether due to suspension, termination, debarring, or other reason for ineligibility. Similarly, such individuals must also disclose if they are at risk of becoming ineligible, under investigation, or facing potential or actual disciplinary action.

Standard 4. Business Relationships and Conflicts of Interest Avoidance

- **Gifts:** Applicable Individuals are not permitted to solicit or accept gifts, favors, services, entertainment, or other items of value from any entity that provides items or services which may be used by CHPIV. Attending business meetings at which meals are served is considered a permissible activity.
- **Business Inducements:** Applicable Individuals are prohibited from using their positions to personally profit or assist others in profiting in any way. This includes improper use of business courtesies, payments, and offering, giving, soliciting, or receiving any form of bribe or improper payment.
- **Conflict of Interest:** Conflicts of Interests, as well as the appearance of a Conflicts of Interest, must be avoided. Applicable Individuals must comply with applicable Conflict of Interest Laws, including California Government Code 1090 et seq., California Political Reform Act (Government Code Section 81000 et seq.) and common conflict of interest laws. Additionally, Applicable Individual must avoid actions or relationships that can appear to influence the individual's ability to perform their duties objectively. Examples of conflicts of

Interest include but are not limited to seek employment as a director, officer, or consultant with or hold financial interest in any competitor, vendor, or health care provider; personal gain through access to company information; accepting gifts or favors from an outside company that does business with CHPIV; etc. CHPIV requires any potential or actual conflicts of interest to be reported to the Chief Compliance Officer. Prior written approval of the CEO, or in the case of the CEO, the Chair of the Commission, must be provided should an employee seek to perform work for any organization with which CHPIV does business/seeks to do business, be a director, officer, or consultant of any contractor, or permit their name to be used such that it indicates a business connection with any contractor. CHPIV will take action to eliminate the Conflict of Interest, up to and including separation from employment.

Standard 5. Public Entity Integrity

- **Use of Public Funds:** CHPIV complies with applicable laws regarding investment of public funds and expenditure limits. Applicable Individuals are prohibited from using public funds or assets for gifts or lending of credit to private persons without adequate consideration unless such actions clearly serve a public purpose consistent with CHPIV's mission and authority. Such use of funds must also be approved by CHPIV's legal counsel.
- **Public Meetings:** CHPIV and its Commission must comply with the Ralph M. Brown Act, California Government Code Sections 5490 et seq with regard to public meetings.

Standard 6. Record Keeping and Confidentiality

- **Books and Records:** CHPIV, a public entity, is subject to the California Public Records Act, California Government Code Sections 6250 et seq. (CPRA). As such, CHPIV records or copies of records may be viewed by members of the public, unless the information is protected from disclosure under the CPRA. If you receive a CPRA-related request, please refer the requestor to Compliance@chpiv.org.
- All CHPIV records, documents, and data, whether hard copy or electronic, must be preserved in accordance with applicable regulations and CHPIV policies.
- CHPIV requires recordkeeping to be accurate and legal. Alteration or falsification of any CHPIV records is prohibited. This includes financial records. Improper record keeping should be reported immediately to the Chief Compliance Officer (Compliance@chpiv.org).

III. Addressing Noncompliance with the Code of Conduct

In the case of a violation of the Code of Conduct, the Applicable Individual is subject to disciplinary action including termination of employment/contract. Violations of the Code of Conduct include but are not limited to failure to follow CHPIV policies or applicable law; failure to disclose information or giving false information in connection with an investigation; neglecting to address and/or report a violation with the Code of Conduct, policy, or applicable law; or retaliation against an individual who reported a suspected violation.

Potential violations can be reported via the following methods:

Compliance Hotline	800-919-4947
Chief Compliance Officer	Elysse Tarabola, Chief Compliance Officer Email: ETarabola@chpiv.org Direct Line: (760) 232-5021
Compliance Department	Compliance@chpiv.org
Human Resources	Michelle Ortiz, Office & HR Manager Email: MOrtiz@chpiv.org Direct Line: 760-970-5072
Online Reporting Form	chpiv.org/compliance-program

IV. Resources

CHPIV Policies & Procedures Repository

If you need more information or have any questions regarding the information within this Code of Conduct, applicable law, or CHPIV policies, please contact your Compliance or Human Resources departments.

Attestation of Receipt and Acknowledgment of Code of Conduct

Attestation

I, the undersigned, hereby acknowledge that I have received and understood the Code of Conduct of Community Health Plan of Imperial Valley (CHPIV) dated August 14, 2023. I understand that it is my responsibility to read and comply with the policies and guidelines outlined in the Code of Conduct.

The Code of Conduct outlines the expected behaviors, standards, and professional conduct that all employees are expected to adhere to while performing their duties and responsibilities within and on behalf of the company.

Acknowledgement

I acknowledge that:

1. I have received a copy of the Code of Conduct.
2. I understand the expectations and standards as outlined in the Code of Conduct.
3. I am aware that it is my responsibility to seek clarification on any aspects of the Code of Conduct that I do not fully understand.
4. I understand that failure to comply with the Code of Conduct may result in disciplinary action, up to and including termination of my employment or engagement with the company.
5. I am committed to upholding the principles and guidelines outlined in the Code of Conduct to the best of my ability.

Agreement

By signing below, I hereby agree to adhere to and uphold the principles and policies outlined in the Code of Conduct of CHPIV.

Full Name: _____

Position/Title: _____

Signature: _____

Date: _____

This attestation is intended to encourage understanding and adherence to the company's Code of Conduct. It also facilitates a culture of integrity, respect, and professionalism that strengthens the company's reputation and work environment. Thank you for your commitment to upholding CHPIV's Code of Conduct.

	Escalation of Noncompliance Issues	CMP-007
Department	Compliance	
Functional Area	Compliance	
Impacted Delegate	☒ Subcontractor ☐ NA	

DATES			
Policy Effective Date	10/09/2023	**Reviewed/Revised Date**	
Next Annual Review Due	10/09/2024	**Regulator Approval**	08/25/2023

APPROVALS		
Internal		**Regulator**
Name	Elysse Tarabola	☒ DHCS ☐ NA ☒ DMHC
Title	Chief Compliance Officer	

ATTACHMENTS

- NA

AUTHORITIES/REFERENCES

- CMP-001 Corrective Action Plan
- CHPIV Compliance Program and Plan
- CHPIV Delegation Oversight Program
- CHPIV Contract with Department of Healthcare Services (DHCS)
- Delegation Agreements
- Department of Health Care Services All-Plan Letter (APL) 17-004: Subcontractual Relationships and Delegation
- Title 42, Code of Federal Regulations (C.F.R.), §438.230

HISTORY

Revision Date	Description of Revision
10/09/2023	Policy creation

I. OVERVIEW

A. The purpose of this policy is to establish a clear and structured framework for handling noncompliance issues within Community Health Plan of Imperial Valley (CHPIV). Noncompliance refers to instances where MEMBERS, providers, or employees fail to adhere to the established rules, regulations, and policies, which may lead to potential risks or disruptions in the provision of healthcare services. This policy aims to address noncompliance promptly and efficiently while promoting transparency, fairness, and compliance with all applicable laws and regulations.

II. POLICY

A. The policy ensures a systematic approach to identify, report, investigate, and resolve noncompliance issues promptly and effectively. By following this policy, we aim to uphold the highest standards of ethics, quality of care, and compliance with all relevant laws and regulations.

III. PROCEDURE

A. Identification of Noncompliance: Noncompliance issues may arise from DELEGATED ENTITIES, providers, or employees failing to follow established policies, contractual obligations, ethical guidelines, or relevant laws and regulations. Noncompliance can be identified through AUDITS, MONITORING, feedback from MEMBERS and providers, or self-reporting.

B. Reporting Noncompliance: Any individual who becomes aware of a noncompliance issue must report it immediately to their immediate supervisor, any MEMBER of the leadership team, Chief Compliance Officer, or Compliance department. Anonymous reporting is available through the CHPIV website and Compliance Hotline.

C. Initial Assessment: Upon receiving a report of noncompliance, the Compliance department shall conduct an initial assessment to determine the severity and legitimacy of the reported issue.

D. Investigation: The Compliance department will lead a formal investigation, document findings, and require a CORRECTIVE ACTION PLAN, as appropriate.

E. Executive Management Involvement: All compliance issues will be escalated to the Chief Compliance Officer. Compliance issues that pose a significant risk to CHPIV's integrity will be brought to the attention of the Chief Executive Officer for discussion. Upon the Chief Executive Officer's agreement, the Compliance Issue will progress through successive levels of escalation, involving the COMPLIANCE & POLICY COMMITTEE, Leadership Team, the Commission, and the regulatory agencies. Additionally, the CCO has the authority and direct access to the Commission should they choose to escalate matters directly at that level.

F. Self-Disclosures to Regulatory Agencies: CHPIV encourages a culture of transparency and self-policing. If noncompliance issues identified have regulatory implications, CHPIV is responsible for self-disclosing matters to the appropriate regulatory authorities.

G. Training: Employees may undergo training related to the noncompliance.

H. Corrective Action Plans: CORRECTIVE ACTION PLANS are required to correct noncompliance issues in accordance with CAP requirements set forth in CHPIV P&P CMP-003 CORRECTIVE ACTION PLANS.

1. The elements of the CAP must be resolved in accordance with CHPIV P&P CMP-003: CORRECTIVE ACTION PLANS.
2. In the event the elements of the CAP are not successfully completed within ninety (90) calendar days, the Compliance department shall report to the CPC following the CAP period. CPC will review the outstanding CAP items to determine, at its discretion, whether the CAP deadline should be extended.
    a. The Compliance Department must demonstrate to the reasonable satisfaction of the CPC the reason for such an extension and provide a detailed, step action plan to ensure that the items for correction are being addressed in a timely manner.
3. CORRECTIVE ACTION PLANS are monitored in accordance with CHPIV P&P CMP-003: CORRECTIVE ACTION PLANS.

I. Disciplinary actions: CHPIV may impose progressive disciplinary actions with consistent performance issues or findings regarding significant compliance issues.

1. Staff: In addition to CORRECTIVE ACTION PLANS, noncompliance issues involving CHPIV staff may result in the following disciplinary actions:
    a. Additional Training: Employees may undergo additional training related to the violation.
    b. Verbal and Written Warnings: For minor noncompliance, a verbal and written warning will be issued to remind the employee of the expected standards of conduct, outlining the violation and potential consequences.
    c. Probationary Period: Serious or repeated noncompliance may result in probation with close MONITORING for improvement.
    d. Suspension: Significant noncompliance may lead to a temporary suspension as a serious warning.
    e. Termination: Severe or repeated noncompliance may lead to employment termination.
2. Noncompliance issues and disciplinary actions related to DELEGATED ENTITIES are further outlined in P&P CMP-002 Delegation Oversight.

IV. DEFINITIONS

Whenever a word or term appears capitalized in this policy and procedure, the reader should refer to the "Definitions" below.

TERM	DEFINITION
Auditing	A Systematic evaluation of performance to ensure consistency with ethical standards, federal or state statute, regulations, policies, contractual obligations and National Committee for Quality Assurance

TERM	DEFINITION
	(NCQA) requirements. 1. External Audit – Evaluation of CHPIV as conducted by an external regulatory or accreditation body; 2. Internal Audit – Evaluation of CHPIV operational areas, department, or systems as conducted by Regulatory Affairs and Compliance (RAC); or 3. Oversight Audit – Evaluation of delegate/SUBCONTRACTOR as conducted by CHPIV, at least annually.
Compliance & Policy Committee (CPC)	An internal committee comprised of CHPIV management staff that monitors compliance activities and makes recommendations for action to CHPIV staff, including CHPIV's executive staff, and the Commission.
Corrective Action Plan (CAP)	A plan delineating specific identifiable activities or undertakings that address and are designed to correct program deficiencies or problems identified by formal audits or monitoring activities by CHPIV, the Centers for Medicare & Medicaid Services (CMS), Department of Health Care Services (DHCS), or designated representatives. FDRs and/or CHPIV departments may be required to complete CAPs to ensure compliance with statutory, regulatory, or contractual obligations and any other requirements identified by CHPIV and its regulators.
Delegated Entity (Delegate)	A contracted entity which CHPIV authorizes to perform certain functions on its behalf. Although, CHPIV can delegate the authority to perform a function, it cannot delegate the responsibility for ensuring that the function is performed according to CHPIV and National Committee on Quality Assurance (NCQA) standards.
Delegation Agreement	Mutually agreed upon document, signed by both parties, which includes, without limit: 1. CHPIV responsibilities; 2. Duration of the agreement; 3. Termination of the agreement; 4. Delegated Entity responsibilities and Delegated Services; 5. Types and frequency of reporting to the Delegated Entity; 6. Process by which the CHPIV evaluates the Delegated Entity's performance (Performance Measurements); 7. Use of confidential CHPIV information including Member Protected Health Information (PHI) by the Delegated Entity; and 8. Remedies available to the CHPIV if the Delegated Entity does not fulfill its obligations.
Member	A beneficiary enrolled in a CHPIV program.
Monitoring	The mechanism for ongoing collection and review of performance data against benchmarks derived from statues, regulations, policy, contractual obligations, and/or NCQA standards.

QUIZ

1. You discover an unattended email address or fax machine in your office receiving beneficiary appeals requests. You suspect no one is processing the appeals. What should you do?

    a. Contact law enforcement

    b. Contact your compliance department (via compliance hotline or other mechanism)

    c. Wait to confirm someone is processing the appeals before taking further action

    d. Do nothing

2. A sales agent, employed by the Sponsor's first-tier, downstream, or related entity (FDR), submitted an application for processing and requested two things 1) to back-date the enrollment date by one month, and 2) to waive all monthly premiums for the beneficiary.
What should you do?

    a. Refuse to change the date or waive the premiums but decide not to mention the request to a supervisor or the compliance department.

    b. Make the requested changes because the sales agent determines the beneficiary's start date and monthly premiums.

    c. Tell the sales agent you will take care of it but then process the application properly (without the requested revisions)—you will not file a report because you don't want the sales agent to retaliate against you.

    d. Process the application properly (without the requested revisions)—inform your supervisor and the compliance officer about the sales agent's request.

3. You work for a Sponsor. Last month, while reviewing a Centers for Medicare & Medicaid Services (CMS) monthly report, you identified multiple individuals not enrolled in the plan but for whom the Sponsor is paid. You spoke to your

supervisor who said don't worry about it. This month, you identify the same enrollees on the report again. What should you do?

   a. Decide not to worry about it as your supervisor instructed—you notified your supervisor last month and now it's their responsibility.

   b. Although you know about the Sponsor's non-retaliation policy, you are still nervous about reporting—to be safe, you submit a report through your compliance department's anonymous tip line to avoid identification.

   c. Wait until the next month to see if the same enrollees appear on the report again, figuring it may take a few months for CMS to reconcile its records—if they are, then you will say something to your supervisor again.

   d. Contact law enforcement and CMS to report the discrepancy.

4. Compliance is only the responsibility of the Compliance Officer, Compliance Committee, and Upper Management.

   a. True

   b. False

5. Ways to report a compliance issue include:

   a. Telephone hotlines

   b. Report on the Sponsor's website

   c. In-person reporting to the compliance department/supervisor

   d. All of the answers

6. What is the purpose of the non-retaliation policy?

   a. Allows the Sponsor to discipline employees who violate the Code of Conduct.

   b. Prohibits management and supervisor from harassing employees for misconduct.

   c. Protects employees who, in good faith, report suspected non-compliance.

   d. Prevents fights between employees.

7. There are examples of issues that can be reported to a Compliance Department: suspected fraud, waste, and abuse (FWA), potential health privacy violations, unethical behavior/employee misconduct, and:

a. Marking inappropriate incentives to members to join certain Medical Groups and/or Health Plans.

b. Documentation and timeliness issues.

c. Quality of care issues.

d. All of the answers including many other high risk areas.

8. Once a corrective action plan begins addressing non-compliance or fraud, waste, and abuse (FWA) committed by a Sponsor's employee or first-tier, downstream, or related entity's (FDR's) employee, ongoing monitoring of the corrective actions is not necessary.

    a. True – management can be trusted to always ensure the plan of correction is implemented.

    b. False – internal monitoring is essential for corrective action plan follow-up.

    c. False – ongoing monitoring is not required by federal or state laws.

    d. True – the organization must report to CMS only.

9. Commercial, Medicare Parts C and D Plan Sponsors are not required to have a compliance program.

    a. True – a compliance program is not required if they have a Quality and Ethics committee.

    b. False – a compliance program is required and must include measures to prevent, detect, and correct non-compliance as well as fraud, waste, and abuse.

    c. True – a compliance program is not required if compliance training is provided every 2 years.

    d. True – a compliance program is only needed if they have commercial customers.

8. Once a corrective action plan begins addressing non-compliance or fraud, waste, and abuse (FWA) committed by a Sponsor's employee or first-tier, downstream, or related entity's (FDR's) employee, ongoing monitoring of the corrective actions is not necessary.

    a. True – management can be trusted to always ensure the plan of correction is implemented.

    b. False – internal monitoring is essential for corrective action plan follow-up.

    c. False – ongoing monitoring is not required by federal or state laws.

d. True – the organization must report to CMS only.

9. Commercial, Medicare Parts C and D Plan Sponsors are not required to have a compliance program.

    a. True – a compliance program is not required if they have a Quality and Ethics committee.

    b. False – a compliance program is required and must include measures to prevent, detect, and correct non-compliance as well as fraud, waste, and abuse.

    c. True – a compliance program is not required if compliance training is provided every 2 years.

    d. True – a compliance program is only needed if they have commercial customers.

12. What are some of the consequences for non-compliance, fraudulent, or unethical behavior?

    a. Disciplinary action

    b. Termination of employment

    c. Exclusion from participating in all Federal health care programs

    d. All of the answers

13. Whistleblowers and persons who report in good-faith any suspected violations or issues are protected from retaliation and intimidation.

    a. True

    b. False

14. You are working as a prior authorization nurse reviewer, your team has been short staffed for the past 6 months and there has been a delay in getting denial letters distributed timely. Your co-worker has an upcoming health plan audit and she asked you to quality check the cases that have been selected. Upon review of quality check you see all files are at 100 % compliance with letter distribution. Given the back log you are suspicious and believe it is likely the co-worker has changed dates on the letters to show compliance with mailing. What would you do?

    a. Do nothing and be glad the health plan audit will have a good outcome.

    b. Contact your supervisor and/or compliance department and report your findings and suspicions.

    c. Talk to your co-worker and ask her how she did this as you have several upcoming audits yourself.

d. Ask your friend from the claims department what you should do.

15. When a strong compliance program is established there is less risk to the customer. Benefits of a strong compliance program include all EXCEPT:

    a. Decreased member financial liability

    b. Appropriate access to providers of choice

    c. Decreased barriers to care

    d. Delayed treatment/services

Health Care Fraud, Waste AND Abuse Training Compliance Training

Training Material

Quiz Submission Due: December 11, 2023

Community Health Plan OF IMPERIAL VALLEY

Table of Contents

I. Introduction....3

II. Objectives....3

III. What is Health Care Fraud?....3

IV. What is Health Care Waste?....4

V. What is Health Care Abuse?....5

VI. Difference Between Fraud, Waste and Abuse....5

VII. How to Prevent FWA....5

VIII. Potential FWA Ref Flag for Potential Member Issues....6

IX. Potential FWA Ref Flag for Potential Provider Issues....6

X. Reporting FWA at Community Health Plan of Imperial Valley....6

XI. What Will Happen After Reporting....7

XII. FWA Laws....8

XIII. FWA Laws False Claims Act (FCA)....8

XIV. FWA Laws Anti-Kickback Statute....8

XV. FWA Laws Stark Law....8

XVI. FWA Laws Civil Monetary Penalties Law....9

XVII. FWA Laws Exclusions....9

XVIII. FWA Laws Civil Monetary Penalties....10

XIX. Health Care Laws....10

XX. Health Care Laws California....10

XXI. Disclaimer....11

XXII. APPENIDX....11

I. Introduction

A. Health care fraud can cost TAXPAYERS billions of dollars

1. The Fall 2022 Semiannual Report to Congress (SAR) highlights nearly $1.29 billion in expected recoveries as a result of HHS-OIG audits and investigations conducted during April 1, 2022 to September 30, 2022.
2. Every year, billions of dollars are improperly spent because of fraud, waste and abuse (FWA). It affects everyone—including you. This training helps you detect, correct and prevent FWA.

II. Objectives

A. Identify fraud and abuse

B. Understand fraud and abuse laws & penalties

C. Recognize risk areas or red flags*

D. How to report fraud and abuse

E. What happens after detection

F. Recognize government agencies and partnerships dedicated to fighting fraud and abuse

G. *Red flags are warnings or discrepancies that attract attention to potential fraud and abuse. Although not evidence of fraud and abuse, a pattern of red flags can increase suspicion and justify further investigation.

H. *Red flags can be general or specific to a line of business and should be reported immediately!

III. What is Health Care Fraud

A. **Fraud** is knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud a health care benefit program, or to obtain, by means of fraudulent pretenses, representations, or promises, any of the money of property owned by, or under the custody or control of, any health care benefit program.

B. Examples of Fraud RED FLAG

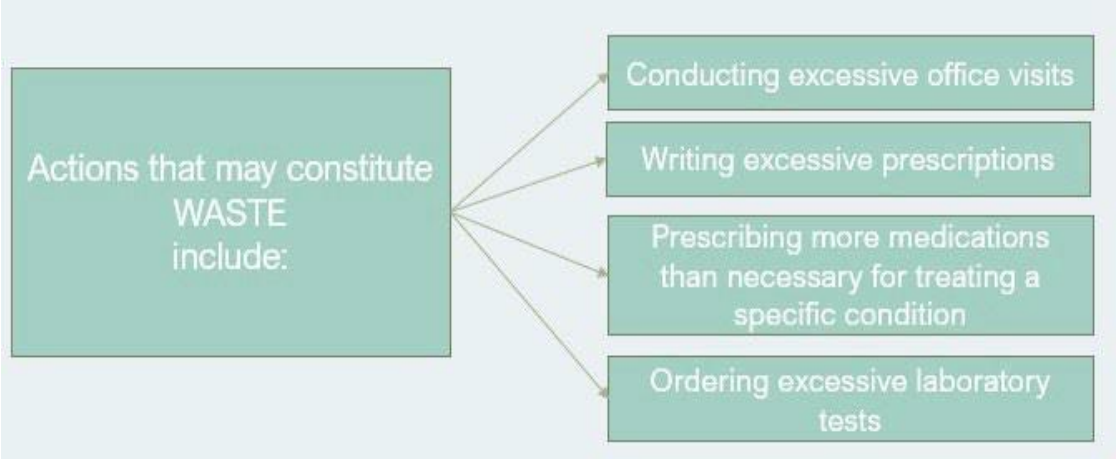
Intentional Act for Gain	FRAUD	Deception	FRAUD
	UM – Making prohibited referrals for certain designated health services.		UM – Falsifying documents to indicate notifications had taken place for approval, modification, or denying a referral request.
	UM – Documenting a verbal denial falsely attributed to a medical professional.		UM – Redirecting care from a contracted provider because of economic profiling (cost) without regulatory approval.
	Staff – Knowingly receiving, offering, and/or paying remuneration to induce or reward referrals for items or services reimbursed by Federal or private health care programs.		Claims – Submitting inaccurate financial reports related to outstanding claims liability.
	Claims – Knowingly submitting, or causing to be submitted, false claims, or making misrepresentations of facts to obtain payment.		Claims – Altering claim audit files to fraudulently show compliance with health plan audits to hide failure to pay claims due to financial insolvency.

IV. What is Health Care Waste

A. **Waste** includes practices that, directly or indirectly, result in unnecessary costs to the Medicare Program, such as overusing services. Waste is generally not considered to be caused by criminally negligent actions but rather by the misuse of resources.

1. For the definitions of fraud, waste and abuse, refer to Section 20, Chapter 21 of the Medicare Managed Care Manual and Chapter 9 of the Prescription Drug Benefit Manual on the Centers for Medicare & Medicaid Services (CMS) website. [mc86c21.pdf (cms.gov)]

2. Examples of Waste RED FLAGS

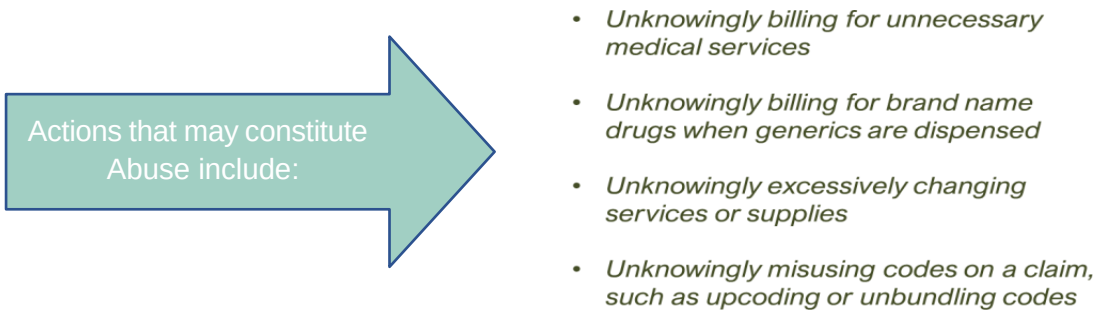


V. What is Health Care Abuse

A. **Abuse** applies to practices that are inconsistent with sound fiscal, business, medical or recipient practices that result in unnecessary cost to a health care program, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. Mistakes that are repeated after discovery or represent an on-going pattern could constitute abuse.

B. Action can directly or indirectly result in unnecessary costs to the Medicare Program.

C. Examples of Abuse RED FLAGS



VI. Differences Between Fraud, Waste and Abuse

A. There are differences among fraud, waste and abuse. One of the primary differences is intent and knowledge.

B. **Fraud** requires intent to obtain payment and the knowledge the actions are wrong.

C. **Waste and Abuse** may involve obtaining an improper payment or creating an unnecessary cost to the Medicare Program but does not require the same intent and knowledge..

VII. How to Prevent FWA

A. Make sure you are up to date with laws, regulations, policies

B. Conduct yourself in an ethical manner

C. Ensure you coordinate with other payers

D. Ensure data/billing is both accurate and timely

E. Know FWA policies and procedures, standards of conduct, laws, regulation

F. Verify information provided to you

G. Be on the lookout for non-compliant activity

H. Be aware of what could be non-compliant activity

VIII. Potential FWA RED FLAGS for Potential Member Issues

A. Make sure you are up to date with laws, regulations, policies

B. Conduct yourself in an ethical manner

C. Ensure you coordinate with other payers

D. Ensure data/billing is both accurate and timely

E. Know FWA policies and procedures, standards of conduct, laws, regulation

F. Verify information provided to you

G. Be on the lookout for non-compliant activity

H. Be aware of what could be non-compliant activity

IX. Potential FWA RED FLAGS for Potential Provider Issues

A. Are the provider's authorization requests appropriate for the member's health condition?

B. Unusual billing practices or suspicious activity

1. Altering dates of services
2. Unbundling or upcoding services

C. Is the provider requesting a higher quantity of a service than medically necessary for the condition?

D. Is the provider's diagnosis for the member supported in the medical records?

X. Reporting FWA at Community Health Plan of Imperial Valley

A. Everyone *must* report suspected instances of FWA. Your Code of Conduct clearly states this obligation. Community Health Plan of Imperial Valley (CHPIV) will not retaliate against you for making a good faith effort in reporting.

B. Report anonymously to Compliance of any FWA.

Compliance Hotline	800-919-4947
Chief Compliance Officer	Elysse Tarabola, Chief Compliance Officer Email: ETarabola@chpiv.org Direct Line: (760) 232-5021
Compliance Department	Compliance@chpiv.org
Online Reporting Form	chpiv.org/compliance-program

C. If warranted, report fraudulent conduct to Government authorities, such as the Office of Inspector General (OIG), the U.S. Department of Justice (DOJ), or CMS. Reporting to CHPIV Compliance will facilitate evaluation of every report to identify if external notification is warranted.

D. Individuals or entities (physicians, companies) who voluntarily disclose a self-discovered potential fraud to OIG may do so under the Self-Disclosure Protocol (SDP). Self-disclosure gives providers the opportunity to avoid the costs and disruptions associated with a Government-directed investigation and civil or administrative litigation.

E. **Do not be concerned about whether it is fraud, waste or abuse**

1. If warranted:

HHS Office of Inspector General:

Phone: 1-800-HHS-TIPS (1-800-447-8477) or TTY 1-800-377-4950

Email: HHSTips@oig.hhs.gov

Online: https://oig.hhs.gov/fraud/report-fraud/

2. For Medicare Parts C and D:

Investigations Medicare Drug Integrity Contractor (I MEDIC) at 1-877-7SafeRx (1-877-772-3379)

3. CMS Hotline at 1-800-MEDICARE (1-800-633-4227) or TTY 1-877-486-2048

XI. What Will Happen After Reporting

A. Once suspected or actual fraud, waste or abuse is detected, work starts promptly to confirm and identify the extent of the issues. Once identified, measures to correct start immediately. Correcting the problem saves the government money and ensures compliance with CMS requirements & other regulatory / governing body.

B. CHPIV will develop a plan to correct the issue. If it does not interrupt the investigation, Compliance Department and Leadership may be able to provide the steps in the development process for the corrective action plan. The actual plan is going to vary, depending on the specific circumstances.

1. Design the corrective action to correct the underlying problem that resulted in FWA program violations and to prevent future noncompliance.
2. Tailor the corrective action to address the specific FWA problem or issues identified. Timelines for actions are important to ensure completion.

3. All corrective actions addressing noncompliance or FWA committed must be documented, including consequences for failure to satisfactorily complete the corrective action.

4. It is necessary to monitor corrective action continuously until the team can ensure the effectiveness of the correction.

XII. FWA Laws

A. **The five most important Federal fraud and abuse laws that apply to physicians are the:**

1. False Claims Act (FCA)
2. Anti-Kickback Statute (AKS)
3. Physician Self-Referral Law (Stark law)
4. Exclusion Authorities
5. Civil Monetary Penalties Law (CMPL)

B. http://oig.hhs.gov/fraud/PhysicianEducation/

XIII. FWA Laws False Claims Act (FCA)

A. **False Claims Act (FCA) prohibits:**

1. Presenting a false claim for payment or approval
2. Making or using a false record or statement in support of a false claim
3. Conspiring to violate the False Claims Act
4. Falsely certifying the type/amount of property to be used by the Government
5. Certifying receipt of property without knowing if it is true
6. Buying property from an unauthorized Government officer
7. Knowingly concealing or knowingly and improperly avoiding or decreasing an obligation to pay the Government
8. 31 United States Code § 3729-3733

XIV. FWA Laws Anti-Kickback Statute

A. **Anti-Kickback Statute (AKS)**

1. Prohibits knowingly and willfully soliciting, receiving, offering or paying remuneration (including any kickback, bribe, or rebate) for referrals for services that are paid in whole or in part under a federal health care program (which includes the Medicare program).
2. 42 United States Code §1320a-7b(b)

XV. FWA Laws Stark Law

A. **Physician Self-Referral Law (Stark law)**

1. Prohibits a physician from making a referral for certain designated health services to an entity in which the physician (or a member of his or her family) has an ownership/investment interest or with which he or she has a compensation arrangement (exceptions apply).
2. 42 United States Code §1395nn

XVI. FWA Laws Civil Monetary Penalties Law

A. Civil Monetary Penalties Law

1. The Office of Inspector General (OIG) may impose civil penalties for several reasons, including:
2. Arranging for services or items from an excluded individual or entity
3. Providing services or items while excluded
4. Failing to grant OIG timely access to reports
5. Knowing of and failing to report and return an overpayment
6. Making false claims
7. Paying influenced referrals

XVII. FWA Laws Exclusions

A. Exclusion

1. No Federal health care program payment may be made for any item or service furnished, ordered, or prescribed by an individual or entity excluded by the Office of Inspector General (OIG). The OIG has authority to exclude individuals and entities from federally funded health care programs and maintains the "List of Excluded Individuals and Entities" (LEIE)
2. The U.S. General Services Administration (GSA) administers the System for Award Management (SAM), which contains debarment actions taken by various Federal agencies, including the OIG. Access to the EPLS is available through the System for Award Management (SAM) website.
3. Department of Health Care Services (DHCS): Medi-Cal maintains the Suspended and Ineligible (S&I) Provider List of health care providers and entities that have been barred from participation in the Medi-Cal program.
4. Exclusions are reviewed prior to hiring or contracting a new employee, temp or consultant and monthly thereafter.
5. Review of monthly exclusions is essential to prevent inappropriate payment to anyone on the exclusion lists.
6. See Policy Fraud, Waste, and Abuse Program (CMP-009)

XVIII. FWA Laws Civil Monetary Penalties

A. **The Office of Inspector General (OIG) may impose <u>civil penalties</u> for several reasons, including:**

1. Arranging for services or items from an excluded individual or entity
2. Providing services or items while excluded
3. Failing to grant OIG timely access to reports
4. Knowing of and failing to report and return an overpayment
5. Making false claims
6. Paying to influence referrals

XIX. Health Care Laws

The False Claims Act
- Statute: 31 U.S.C. §§ 3729–3733

The Anti-Kickback Statute
- Statute: 42 U.S.C. § 1320a–7b(b)
- Safe Harbor Regulations: 42 C.F.R. § 1001.952

The Physician Self-Referral Law
- Statute: 42 U.S.C. § 1395nn
- Regulations: 42 C.F.R. §§ 411.350–.389

The Exclusion Authorities
- Statutes: 42 U.S.C. §§ 1320a–7, 1320c–5
- Regulations: 42 C.F.R. pts. 1001 (OIG) and 1002 (State agencies)

The Civil Monetary Penalties Law
- Statute: 42 U.S.C. § 1320a–7a
- Regulations: 42 C.F.R. pt. 1003

Criminal Health Care Fraud Statute
- Statute: 18 U.S.C. §§ 1347, 1349

XX. Health Care Laws California

A. ***Welfare Institutions Code 14107 [False Claims]*** - Prohibits claim submission, with intent to defraud, to obtain greater compensation than legally entitled.

B. ***Welfare Institutions Code 14107 (a-b) [Anti-Kickback]*** - Solicits or receives any kickback, bribe or rebate to either refer or promise to refer person(s) for services or merchandise.

C. ***CA Penal Code 550(a)(6-7) [False claims]*** - Imposes liability to knowingly make, or cause to be made, any false or fraudulent claim for health care benefit or which was not used by or on behalf of the claimant.

XXI. Disclaimer

A. This course was prepared as a service and is not intended to grant rights or impose obligations. This course may contain references or links to statutes, regulations or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. Readers are encouraged to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

XXII. APPENIDX

1. Fraud, Waste, and Abuse Program Policy (CMP-009)

	Fraud, Waste, and Abuse Program	CMP-009
Department	Compliance	
Functional Area	Compliance	
Impacted Delegate	☒ Subcontractor ☐ NA	

DATES			
Policy Effective Date	10/9/2023	Reviewed/Revised Date	
Next Annual Review Due	10/9/2024	Regulator Approval	8/25/2023

APPROVALS		
Internal		**Regulator**
Name	Elysse Tarabola	☒ DHCS ☐ NA ☐ DMHC
Title	Chief Compliance Officer	

ATTACHMENTS

- NA

AUTHORITIES/REFERENCES

- Program Integrity Requirements - 42 CFR §438.608(a)(4) and §438.608(a)(8)
- DHCS APL 15-026 – Actions Following Notice of Credible Allegation of Fraud
- DHCS APL 17-003 – Treatment of Recoveries Re: Overpayments to Providers
- DHCS APL 21-003 – Medi-Cal Network Provider & Subcontractor Terminations
- PLAN- 2024 DHCS Contract Exhibit A, Attachment III, Subsection 1.3.4.D CHPIV's Obligations Regarding Suspended, Excluded and Ineligible Providers – Actions to be taken where Credible Allegation of Fraud
- PLAN- 2024 DHCS Contract Exhibit E Section 1.3.7.B Federal False Claims Act Compliance and Support – Cooperation with the Office of Attorney Genera Division of Medi-Cal Fraud & Elder Abuse ('DMFEA") and the U.S. Department of Justice ("DOJ") Investigations and Prosecutions
- U.S. Department of Health and Human Services (HHS) Office of Inspector General ("OIG")
- PLAN- 2024 DHCS Contract Exhibit E Section 3.1.6.A.10 Requirements for Network Provider Agreements, Subcontractor Agreements and Downstream Subcontractor Agreements
- Anti-Kickback Regulations – 42 U.S.C.A. § 1320a-7b(b)
- Mail and Wire Fraud – 18 U.S.C. § 1341
- False Claims Act – 31 U.S.C. § 3729 *et seq.*
- Program Fraud Civil Remedies Act – 31 U.S.C. §§ 3801-3812
- Deficit Reduction Act of 2005
- CA False Claims Act - CA Code § 12650 *et seq.*
- HIPAA – 45 CFR, Part 164
- Provider Self-Disclosure Protocol – 63 Fed. Reg. 58, 399-403 (1998)

HISTORY

Revision Date	Description of Revision
10/9/2023	Policy Creation

I. OVERVIEW

A. The purpose of this FRAUD Prevention Program policy (this "Policy) is to ensure compliance with the Fraud Prevention Program requirements in the MEDI-CAL CONTRACT. This Policy applies to CHPIV and its Staff, NETWORK PROVIDERS, SUBCONTRACTORS, DOWNSTREAM SUBCONTRACTORS, and any other individual or entity providing services for CHPIV under the MEDI-CAL CONTRACT. This Policy defines the framework, responsibilities, and guiding principles for identifying fraudulent activities and reducing related health care costs. This policy is intended to: (i) protect CHPIV, its MEMBERS and other stakeholders by preventing, detecting, investigating, and reporting suspected health care FRAUD, WASTE, and ABUSE ("FWA"); and (ii) establish CHPIV's oversight responsibilities of NETWORK PROVIDERS, SUBCONTRACTORS and DOWNSTREAM SUBCONTRACTORS regarding the creation and maintenance of policies and procedures related to the underlying authorities and references set forth above.

B. CHPIV recognizes the importance of protecting the integrity of the Medi-Cal program and is committed to conducting all activities in accordance with high ethical standards and in compliance with all applicable laws and regulations as stated herein. Our Fully Delegated SUBCONTRACTOR is delegated to implement and maintain a fraud prevention program consistent with these standards and requirements outlined within this policy. As such, CHPIV will:

1. Ensure that all Staff, NETWORK PROVIDERS, SUBCONTRACTORS and DOWNSTREAM SUBCONTRACTORS or agents are educated regarding the federal and state false claims laws and the role of such laws in preventing and detecting FWA;
2. Ensure communication of all requirements of this Policy, and referenced obligations, to its NETWORK PROVIDERS, SUBCONTRACTORS, and DOWNSTREAM SUBCONTRACTORS, and will have a process to ensure its NETWORK PROVIDERS, SUBCONTRACTORS, and DOWNSTREAM SUBCONTRACTORS acknowledge receipt and understanding of the requirements contained within this Policy;
3. Perform audits that include reviewing, researching and documenting potential FWA activities within the organization;
4. Ensure identification and investigation of potential FRAUD from reports and referrals;
5. Ensure implementation of a process to conduct timely inquiry into potential violations;
6. Conduct FWA awareness training for Staff;
7. Ensure documentation and retention of all records pertaining to corrective actions imposed as a result of violations;
8. Ensure that NETWORK PROVIDERS, SUBCONTRACTORS and DOWNSTREAM SUBCONTRACTORS have a robust FWA program in place, which includes the requirements of this Policy and ongoing monitoring and mandatory annual training;

9. Fully disclose to State and federal regulatory agencies any FRAUD or misconduct within the Plan, NETWORK PROVIDERS, SUBCONTRACTORS or DOWNSTREAM SUBCONTRACTORS; and
10. Fully cooperate with DHCS, DMFEA, OIG, and DOJ investigations and prosecutions in the event of allegations of FRAUD.

B. Retaliation or intimidation toward the reporter(s) of FWA will be strictly prohibited, and this Policy supports reporting of any such retaliation to the Compliance Officer/Fraud Prevention Officer.

C. CHPIV requires that its SUBCONTRACTORS comply with the requirements and provisions of this Policy and, also, that its SUBCONTRACTORS require in their written contracts with NETWORK PROVIDERS and DOWNSTREAM SUBCONTRACTORS that they comply with the requirements and provisions of this Policy to the extent applicable and required by law or regulation.

II. POLICY

A. Fraud Prevention

1. CHPIV provides a confidential FRAUD hotline for FRAUD reports from Staff, MEMBERS, SUBCONTRACTORS, DOWNSTREAM SUBCONTRACTORS, NETWORK PROVIDERS, and any other individuals with a need to report suspected FRAUD and ensures that its SUBCONTRACTORS provide a confidential FRAUD hotline for FRAUD reports from their staff, MEMBERS, NETWORK PROVIDERS, DOWNSTREAM SUBCONTRACTORS, and any other individuals with a need to report suspected FRAUD.
2. CHPIV provides multiple mechanisms for reporting, including the confidential hotline, Staff exit interview surveys, email reporting, and a dedicated address for submission via U.S. Mail.
3. CHPIV ensures FRAUD prevention activities and suspected FRAUD are reported directly to regulatory and law enforcement agencies as required by law.
4. FRAUD activities and suspected FRAUD identified by NETWORK PROVIDERS, SUBCONTRACTORS and DOWNSTREAM SUBCONTRACTORS are communicated to CHPIV.
5. CHPIV ensures FRAUD and ABUSE Activities include, but are not limited to:
    a. Complying with 42 CFR Part 455, §§ 455.104 (Disclosure by Medicaid providers and fiscal agents: Information on ownership and control), 455.105 (Disclosure by providers: Information related to business transactions), 455.106 (Disclosure by providers: Information on persons convicted of crimes), and 42 CFR section 438.610 (Prohibited affiliations);
    b. Ensure that SUBCONTRACTORS are requiring NETWORK PROVIDERS and DOWNSTREAM SUBCONTRACTORS to enroll and remain enrolled in the Medi-Cal program, to the extent required under the MEDI-CAL CONTRACT;
    c. Ensure that SUBCONTRACTORS are confirming the identity of NETWORK PROVIDERS, and any Person with an Ownership or Control Interest or who is an agent or Managing Employee of a Network Provider, upon contract execution or renewal and credentialing, through routine checks of State and federal databases;

The databases to be checked are the Social Security Administration's Death Master File, the National Plan and Provider Enumeration System (NPPES) and the Excluded Provider Lists maintained by the State;

d. Tracking SUBCONTRACTORS and ensuring SUBCONTRACTORS are tracking NETWORK PROVIDERS and DOWNSTREAM SUBCONTRACTORS through review of the following exclusionary databases and lists no less frequently than monthly and upon contract execution or renewal, and upon provider credentialing, taking appropriate action in accordance with ALL PLAN LETTER (APL) 15-026, and APL 21-003:
    i. List of suspended and ineligible providers located at https://files.medi-cal.ca.gov/pubsdoco/SandILanding.aspx,
    ii. List of OIG Excluded Individuals and Entities (LEIE) located at https://oig.hhs.gov/exclusions/exclusions_list.asp,
    iii. Excluded Parties List System (EPLS) within the HHS System for Award Management (SAM) database located at https://sam.gov/content/home;
e. Ensuring training of Staff, directors, NETWORK PROVIDERS, and SUBCONTRACTORS (and ensuring NETWORK PROVIDERS and SUBCONTRACTORS ensure training of DOWNSTREAM SUBCONTRACTORS) on FRAUD schemes, FRAUD detection and FRAUD prevention activities at least annually. Training may consist of an online course, in-person sessions, and/or distribution of written materials. Training topics will also include:
    i. Federal and State FALSE CLAIMS ACT statutes,
    ii. Federal remedies for false claims and statements,
    iii. State laws containing civil or criminal penalties for false statements
    iv. WHISTLEBLOWER protections,
    v. How to handle instances of suspected health care FRAUD;
f. Ensuring that FRAUD prevention efforts are communicated in provider manuals, NETWORK PROVIDER and MEMBER newsletters, internal newsletters or information blasts, targeted mailings or in-service meetings;
g. Ensuring that a method is maintained to verify, by sampling or other methods, that services that have been represented to have been delivered by NETWORK PROVIDERS were in fact received by MEMBERS (42 CFR §438.608(a)(5)). CHPIV will provide proof of compliance with this requirement when requested by DHCS, in a form and manner specified by DHCS through APL, or other similar instruction.
h. Ensuring that there is monitoring and oversight of activities and reports to detect and deter fraudulent behavior, such as:
    i. MEMBER and provider grievances,
    ii. Claims review, including
        A. Clinical edits for invalid gender, out of normal age range, invalid diagnosis for procedure billed, redundant billing, and others
        B. Billings for non-covered benefits
        C. Claims for ineligible individuals
        D. Reviews for emergency diagnosis, emergency place of service and conformance to the definition of "emergency" and "medical necessity"
        E. Claims pended for review by the Claims Supervisor

1. All claims received from other countries
2. All MEMBER reimbursements for proper documentation,

iii. Medical management audits,
iv. Utilization management activities, including checking out-of-area claims to ensure the MEMBER lives within the service area,
v. Quality management activities,
vi. Operational reviews conducted by CHPIV's internal audit department, including eligibility audits,
vii. Financial audits to ensure compliance with State and federal rules for reinsurance and the identification and return of overpayments;

i. Communicating an email address and an address for U.S. Mail to report suspicious behavior of FWA, confidentially or otherwise. Also, maintaining a toll-free hotline (866)685-8664 for confidential reporting of suspected FRAUD and ABUSE. The hotline is monitored by Staff. All reports of suspected FRAUD received from Staff, NETWORK PROVIDERS, SUBCONTRACTORS, DOWNSTREAM SUBCONTRACTORS, MEMBERS, or other credible sources will be logged, investigated, and tracked;
j. Ensuring investigation and resolution of all reported and/or suspected instances of FRAUD and taking action against confirmed FRAUD, including, but not limited to, reporting to law enforcement agencies as required by the MEDI-CAL CONTRACT, termination of the MEMBER or Staff, termination of the contract with a Network Provider, Subcontractor, or Downstream Subcontractor, and/or removal of a NETWORK PROVIDER from the network;
k. Reporting suspected FRAUD as required under section titled "Reporting" in this Policy;
l. Filing an annual written report with DHCS and DMHC and other entities as required by law of CHPIV's efforts to deter, detect and investigate FRAUD; a log of all cases reported to government agencies; and the number of cases known to be prosecuted;
m. If DHCS, DMFEA, or DOJ, or any other authorized State or federal agency, determines there is a credible allegation of Fraud against a Network Provider, SUBCONTRACTOR or Downstream Subcontractor:
    i. CHPIV complies with the MEDI-CAL CONTRACT, all applicable State and federal laws, APL 15-026, and APL 21-003,
    ii. CHPIV ensures there are procedures in place to ensure immediate suspension of payments to the Network Provider, Subcontractor, or DOWNSTREAM SUBCONTRACTOR for which a State or federal agency determines there is a credible allegation of FRAUD (42 CFR § 438.608(a)(8)),
    iii. CHPIV may conduct additional monitoring, require temporary suspension, and/or termination of the Network Provider, SUBCONTRACTOR or Downstream Subcontractor,
    iv. When DHCS notifies CHPIV that a credible allegation of FRAUD has been found against a provider relating to provision of Fee-For-Service Medi-Cal services and that provider is also a Network Provider, one or more of the following four actions must be taken with submission of all supporting documentation to the MCQMD@dhcs.ca.gov inbox

A. Termination of the NETWORK PROVIDER from the network
B. Temporary suspension of the NETWORK PROVIDER from the network pending resolution of the FRAUD allegation
C. Temporary suspension of payment to the NETWORK PROVIDER pending resolution of the FRAUD allegation, and/or
D. Additional monitoring, including audits of the Network Provider's claims history and future claims submissions for appropriate billing,

v. CHPIV must notify DHCS as to which of the above four actions are taken. No action will be required that would interfere with State or federal criminal investigations,
vi. In the event of a Network Provider, Subcontract or, or DOWNSTREAM SUBCONTRACTOR termination, CHPIV will ensure all the requirements and guidance listed in APL 21-003: Medi-Cal NETWORK PROVIDER and SUBCONTRACTOR Terminations are followed,
vii. CHPIV will fully cooperate in any investigation or prosecution conducted by the DMFEA and the DOJ. CHPIV's cooperation must include without limitation
A. Providing upon request, information, and access to records, and
B. Making available Staff or, to the extent appropriate, SUBCONTRACTOR for in-person interviews, consultation, grand jury proceedings, pre-trial conference, depositions, and hearings at DHCS headquarters in Sacramento,
viii. CHPIV litigation support for CMS, DMFEA, and other agencies includes
A. Ensuring that NETWORK PROVIDERS timely gather, preserve, and provide to DHCS, CMS, DMFEA, and any authorized State or federal regulatory agencies, any records in Network Provider's possession, and
B. Ensuring that SUBCONTRACTORS and DOWNSTREAM SUBCONTRACTORS timely gather, preserve, and provide to DHCS, CMS, DMFEA, and any authorized State or federal regulatory agencies, any records in their possession.

6. CHPIV's expectations of NETWORK PROVIDERS and SUBCONTRACTORS for FRAUD prevention and detection include, but are not limited to:
a. Developing a FRAUD program, implementing FRAUD prevention activities, and communicating such program and activities to its DOWNSTREAM SUBCONTRACTORS consistent with this Policy.
b. Training staff, employed and contracted health care providers, including but not limited to physicians and other affiliated or ancillary providers and DOWNSTREAM SUBCONTRACTORS on FRAUD prevention activities at least annually, and ensuring that its DOWNSTREAM SUBCONTRACTORS also comply with this provision in any further downstream agreements.
c. Communicating FRAUD awareness, including identification of FRAUD schemes, detection methods and monitoring activities, to internal personnel, DOWNSTREAM SUBCONTRACTORS, and CHPIV.
d. Notifying CHPIV of suspected fraudulent behavior.
e. Taking action against suspected or confirmed FRAUD, including referring such instances to law enforcement and reporting activity to CHPIV.
f. Cooperating with CHPIV in FRAUD detection and awareness activities, including

monitoring and reporting.

B. Administration

1. CHPIV ensures all potential FWA cases are logged, investigated, and monitored.
2. CHPIV's Fully Delegated Subcontractor's Compliance Officer/Fraud Prevention Officer shall attend and participate in DHCS's quarterly integrity meetings, as scheduled.
3. CHPIV ensures DHCS is notified of any changes in Member's circumstances that impact Medi-Cal coverage pursuant to Medi-Cal program eligibility requirements, including changes in the Member's residence, income, insurance status, and death (42 CFR § 438.608(a)(3)) in a form and manner specified by DHCS through APL or other similar instructions.
4. CHPIV ensures a report of potential instance of FWA is received, an inquiry is initiated as expeditiously as reasonably necessary, but no later than two weeks after the date that the potential misconduct is reported.
    a. If an individual believes that the response to his or her report is completed within a reasonable period of time, he or she is required to bring the matter to the attention of the Compliance Officer/Fraud Prevention Officer.
    b. Failure to report and disclose, or assist, in an investigation of FWA is a breach of the duty that all Staff have to CHPIV and CHPIV's Fully Delegated SUBCONTRACTOR and may result in disciplinary action, up to and including termination.
        i. The CHPIV Compliance Hotline number is (866) 685-8664.
        ii. Written reports may be mailed to: Centene Special Investigations Unit 7700 Forsyth Blvd. Clayton, MO 63105.
5. Files containing investigation materials must be kept in a confidential locked and secured location. Files must be retained a minimum of ten (10) years, unless a longer period of time is required by law or regulation.
6. All parties to the investigation: MEMBERS, NETWORK PROVIDERS, SUBCONTRACTORS, DOWNSTREAM SUBCONTRACTORS, Staff MEMBERS or others named in any form or fashion within the investigation are to be kept confidential to the extent allowable by law.
7. All parties having information relating to the subject of the investigation must hold all information strictly confidential to the extent allowable by law; failure to do so will result in disciplinary action up to and including termination.
8. CHPIV protects as "confidential information" all information shared by or received from DHCS, other State agencies, and federal agencies, and other Medi-Cal managed care plans in connection with any FWA referral, until formal criminal proceedings are made public. CHPIV receives the confidential information as a DHCS business associate in order to facilitate CHPIV's contractual obligations to maintain a FWA prevention program. PHCIV receives and maintains this confidential information in its capacity as a Medi-Cal managed care plan and uses such confidential information only for conducting an investigation into any potential FWA activities and in furtherance of any other program integrity activities.
9. Preliminary and quarterly reports are to be kept confidential and submitted to the DHCS Program Integrity Unit.
10. In the event CHPIV is required to share investigative information with a Network Provider, Subcontractor, or Downstream Subcontractor, CHPIV ensures that the Network Provider, Subcontractor, or DOWNSTREAM SUBCONTRACTOR acknowledges and

agrees that such information will be kept confidential by the Network Provider, Subcontractor, or Downstream Subcontractor.

C. Investigations

1. CHPIV ensures a complete investigation is conducted for all FWA referrals received from DHCS, other State agencies, federal agencies, and other Medi-Cal managed care plans, relating to CHPIV's NETWORK PROVIDERS, SUBCONTRACTORS, and DOWNSTREAM SUBCONTRACTORS. CHPIV submits to DHCS a completed investigation report and a quarterly status report, as set forth in this policy or otherwise required by DHCS in connection with all DHCS, State and federal agency, and Medi-Cal managed care plan referrals of FWA.
2. CHPIV ensures the prompt and thorough investigation of actual or potential FWA, and requires all Staff to assist in such investigations. Investigations may include but not be limited to the following activities:
    a. On-site visits to NETWORK PROVIDERS and SUBCONTRACTORS.
    b. On-site visits to CHPIV MEMBER homes. These visits could be accomplished in conjunction with the audit and/or medical review Staff, or State survey and certification Staff.
    c. Telephone calls or written questionnaires to a sample of CHPIV MEMBERS asking them to confirm the services they received.
    d. Telephone calls or written questionnaires to providers confirming the need for the services rendered.
    e. Telephone calls, correspondence or on-site visits to other pertinent entities.
3. The Compliance Officer/Fraud Prevention Officer must conclude investigations of potential misconduct within a reasonable time period after discovery of the alleged fraudulent activity and complete a FWA Investigation Report form.
4. Unless otherwise specified, the Compliance Officer/Fraud Prevention Officer shall complete a FWA Investigation Report form that includes, to the extent available, the following:
    a. Plan name, organization, and contact information for follow up
    b. Summary of the issue including
        i. The basic who, what, when, where, how, and why
        ii. Any potential legal violations
    c. Specific statutes and allegations including
        i. A list of civil, criminal, and administrative code or rule violations, State and federal
        ii. A detailed description of the allegations or pattern of FWA
    d. Incidents and Issues including
        i. A list of incidents and issues related to the allegations
    e. Background information
        i. Contact information for the complainant, the perpetrator or subject of the investigation, and beneficiaries, pharmacies, providers, or other entities involved
        ii. Additional background information that may assist investigators, such as names and contact information of informants, relators, witnesses, websites, geographic locations, corporate relationships, networks
        iii. The legal and administrative disposition of the case, if available, including

actions taken by law enforcement officials to whom the case has been referred

f. Perspectives of interested parties
    i. Perspective of CHPIV, DHCS, CMS, Member, and other interested parties
g. Data
    i. Existing and potential data sources
    ii. Graphs and trending
    iii. Maps
    iv. Financial impact estimates
h. Recommendations in pursuing the case
    i. Next steps, special considerations, cautions.

5. Within no more than ten (10) working days of completing the investigation, CHPIV shall submit to DHCS reports signed by an executive officer of CHPIV.
    a. Such prompt reporting demonstrates CHPIV's good faith efforts and willingness to work with the government to correct and remedy the problem. CHPIV will also make good faith efforts to cooperate with law enforcement regarding any misconduct reported to the government, including FRAUD and ABUSE.
    b. If an investigation results in a reasonably suspected case of FWA, or confirms that an incident of FWA has been committed, CHPIV will report the incident as deemed appropriate and required by law or regulation to the following government agencies:
        i. CMS
        ii. OIG (Medicare/Medicaid FRAUD)
        iii. California Department of Justice, Bureau of Medi-Cal FRAUD
        iv. California Department of Health Care Services, Program Integrity Unit
        v. California Department of Managed Health Care (DMHC)
        vi. Medical Board of California or other professional licensing regulatory body
        vii. Local law enforcement agencies
        viii. California Health Benefits Exchange
6. The Compliance Officer/Fraud Prevention Officer, with the assistance of legal counsel, review the case and determine if the reported allegation is a violation of State law, federal law, and/or CHPIV Code of Conduct.
7. CHPIV ensures appropriate corrective actions (for example, repayment of overpayments and disciplinary actions against responsible individuals) are taken in response to the potential violation referenced above.
    a. If an overpayment is of significant magnitude (to be determined on a case by case basis), legal counsel will be sought to determine if self-disclosure to a relevant regulatory agency is warranted.
        i. CHPIV has a duty to promptly conduct a reasonable inquiry upon receipt of information that a potential overpayment has occurred. Failure to make reasonable inquiry may be found to be reckless disregard or deliberate ignorance of the overpayment. When overpayment is identified, the Compliance Officer/Fraud Prevention Officer must report the overpayment to DHCS within 60 calendar days after the date on which the overpayment was identified (the 60-day clock does not start running until after CHPIV's

Fully Delegated SUBCONTRACTOR has had an opportunity to undertake reasonable inquiry into the basis of the alleged overpayment).

b. All overpayments should be reported using the self-reported overpayment refund process (SRORP).
c. The Compliance Officer/Fraud Prevention Officer must provide DHCS and/or CMS, in writing, the following information:
    i. Reason for overpayment (incorrect service date, duplicate payment, incorrect CPT code, insufficient documentation, lack of medical necessity, etc.)
    ii. How the error was identified
    iii. Claim number, as appropriate
    iv. Description of the corrective action plan to ensure the error does not occur again
d. CHPIV must report and refund overpayments received during the prior ten (10) years, and in accordance with APL 17-003 and the MEDI-CAL CONTRACT. CHPIV must comply with guidelines issued by DHCS pertaining to retention policies for the treatment of recoveries of all overpayments from CHPIV to a provider, including the treatment of recoveries of overpayments due to FWA.
e. The Claims Department or its delegate must send a letter, accompanied by supporting documentation, to the person who received an overpayment, recognizing the overpayment and providing a date on which the appropriate funds must be returned. The funds must be returned to CHPIV within 60 calendar days after the date on which the overpayment is identified.
f. Failing to report or return overpaid funds within the required timeframe may result in liability under the FALSE CLAIMS ACT and civil monetary penalties up to and including exclusion from participation in federal health care programs. An overpayment which is properly reported and explained, but is not timely repaid, will not give rise to FALSE CLAIMS ACT liability, unless there is evidence of improper avoidance.

D. Reporting

1. In accordance with 42 CFR § 438.608(a)(7), CHPIV ensures all FWA activities are referred, investigated, and reported to DHCS' Program Integrity Unit (PIU), in a manner prescribed by PIU as follows:

a. Preliminary FWA Reports: CHPIV files a preliminary report with DHCS' PIU detailing any suspected FWA identified by or reported to CHPIV, its NETWORK PROVIDERS, SUBCONTRACTORS, or its DOWNSTREAM SUBCONTRACTORS within ten working days of CHPIV's discovery or notice of such FWA. CHPIV submits a preliminary report in accordance with requirements set forth in an APL or other similar instructions. Subsequent to the filing of the preliminary report, a complete investigation of all reported or suspected FWA activities is promptly conducted;
b. Completed Investigation Report: Within ten working days of completing the FWA investigation (including both CHPIV-initiated and DHCS-initiated referrals), CHPIV submits a completed report to DHCS' PIU. This report includes CHPIV's findings, actions taken, and all documentation necessary to support any action taken by

PCHPIV, and any additional documentation as requested by DHCS or other State and federal agencies;

c. Quarterly FWA Status Report: CHPIV submits a quarterly report to DHCS' PIU on all FWA investigative activities ten working days after the close of every calendar quarter. The quarterly report contains the status of all preliminary, active, and completed investigations, and both CHPIV-initiated and DHCS-initiated referrals. In addition to quarterly reports, CHPIV provides updates and available documentation as DHCS may request from time to time;

d. Manner of Report Submission: CHPIV electronically submits all FWA reports in a form and manner specified by DHCS through APL, or other similar instructions. The required report submission includes without limitation the preliminary FRAUD report, the completed investigation report, and the quarterly status report, including all supporting documents, and any additional documents requested by DHCS.

E. Disciplinary Guidelines and Enforcement

1. CHPIV is committed to communicating clear and concise standards as well as executing the disciplinary process when required.

2. Any employee included in suspected violation of the Compliance Program (including its Fraud Prevention Program, Code of Conduct, policies and procedures), laws, regulations or other types of misconduct, is expected to cooperate fully with the investigation process and assist in its resolution.

3. CHPIV prohibits retaliation against any individual who reports suspected violations to the Compliance Program (including its Fraud Prevention Program, Code of Conduct, policies, and procedures), laws, regulations, or other types of misconduct.

4. Anyone who knowingly violates the Compliance Program (including its Fraud Prevention Program, Code of Conduct, policies and procedures), laws, regulations or other types of misconduct, will be subject to disciplinary action up to and including termination of employment criminal or civil prosecution, and or monetary penalties.

5. Discipline and corrective action shall be applied and enforced consistently, fairly, and without prejudice, in a timely manner. Disciplinary action will be based on the seriousness of the violation. The following activities may lead to disciplinary action up to and including termination of employment or termination of a contract with contracted Staff:

a. A Staff member authorizes or participates in actions that knowingly violate CHPIV's Compliance Program (including its Fraud Prevention Program, Code of Conduct, policies and procedures), or laws or regulations;

b. A Staff member deliberately provides misleading information about violations of the Fraud Prevention Program, Code of Conduct, policies or procedures, or laws or regulations;

c. A Staff member fails to report suspected or known violations of the Fraud Prevention Program and/or Code of Conduct;

d. A Staff member is found to have engaged in intentional or reckless non-compliance;

e. A manager's or supervisor's actions reflect inadequate supervision or lack of diligence regarding violations of the Fraud Prevention Program and/or Code of Conduct, policies or procedures, or laws or regulations; and/or

f. Any manager or supervisor retaliates, directly or indirectly, or encourages others to retaliate against an associate who reports a violation of the Fraud

Prevention Program and/or Code of Conduct, policies or procedures, or laws or regulations.

6. NETWORK PROVIDERS, SUBCONTRACTORS, and DOWNSTREAM SUBCONTRACTORS also have the duty to follow the Fraud Prevention Program and Code of Conduct or similar standards that comply with all laws and regulations and to report any potential non-compliant, unethical, or fraudulent behavior without the fear of retaliation. Failure to comply may result in corrective or disciplinary action up to and including termination of a NETWORK PROVIDER or termination of a contract with a SUBCONTRACTOR or Downstream Subcontractor, and/or referral to governmental authority.
7. The Compliance Officer/Fraud Prevention Officer and the Compliance Committee shall be responsible for determining appropriate corrective action after being informed, briefed, and fully reviewing a complaint regarding potential FRAUD. The Compliance Officer/Fraud Prevention Officer and the Compliance Committee are responsible for all discipline or corrective actions relating to serious violations of the Code, policies or procedures, laws and regulations or other acts of wrongdoing, including possible criminal or civil FRAUD activities.
8. Expectations and disciplinary guidelines are well publicized through a variety of methods, including, but not limited to: the Code of Conduct, supporting policies and procedures, Compliance Program, Fraud Prevention Program, training (including Compliance, FWA, and HIPAA), CHPIV's policy CMP-007 Escalation of Noncompliance Issues.
9. Disciplinary records are retained for a period of ten (10) years, unless a longer time period is required by law or regulation, and reviewed periodically to ensure disciplinary actions are appropriate to the violation and consistently administered.

III. PROCEDURE

A. Delegation Oversight

1. CHPIV delegates the Fraud Prevention Program to its SUBCONTRACTOR, Health Net.
2. CHPIV shall provide oversight and continually assess the delegated functions, responsibilities, processes, and performance of Health Net. CHPIV ensures Health Net's compliance with regulatory and contractual requirements through the following activities which are detailed in *CHPIV Policy CMP-002: Delegation Oversight Policy and Procedure*:
   a. Ongoing monitoring
   b. Performance reviews
   c. Data analysis
   d. Utilization of benchmarks, if available
   e. Annual desktop and on-site audits

IV. DEFINITIONS

Whenever a word or term appears capitalized in this policy and procedure, the reader should refer to the "Definitions" below.

TERMS	DEFINITION
Abuse	Practices that are inconsistent with sound fiscal and business practices

TERMS	DEFINITION
	or medical standards, and result in an unnecessary cost to the Medi-Cal 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 Member practices that result in unnecessary cost to the Medi-Cal program.
All Plan Letter (APL)	The means by which Medi-Cal Managed Care conveys information or interpretation of changes in policy or procedures at the Federal or State levels. APLs provide instruction, if applicable, on how to implement changes on an operational basis.
Downstream Subcontractor	Means an individual or an entity that has a Downstream SUBCONTRACTOR Agreement with a SUBCONTRACTOR or a Downstream Subcontractor. A Network Provider is not a Downstream SUBCONTRACTOR solely because it enters into a Network Provider Agreement.
False Claims Act (FCA)	Federal and state statutes that generally prohibit making, using, or presenting a false statement or document in order to get the federal or state government to pay money. It also applies where false statements or documents are used to avoid paying money to the Government that would otherwise be owed, or for failing to identify and return an overpayment.
Fraud	As defined in Title 42 Code of Federal Regulations (section 455.2) fraud is, "An intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to himself or some other person. It includes any act that constitutes fraud under applicable federal or state law." Fraud also includes potential violations or activities prohibited by applicable federal or state laws including, without limitation, the Federal False Claims Act, 31 U.S.C. Sections 3729-3731 and the California False Claims Act, California Government Code, Sections 12650 – 12656.
Member	A beneficiary enrolled in a CHPIV program.
Network Provider	Provider or entity that has a Network Provider Agreement with Contractor, Contractor's Subcontractor, or Contractor's Downstream Subcontractor, and receives Medi-Cal funding directly or indirectly to order, refer, or render Covered Services under this Contract. A Network Provider is not a SUBCONTRACTOR or Downstream SUBCONTRACTOR by virtue of the Network Provider Agreement.
Subcontractor	An individual or entity that has a subcontract with the MCP that relates directly or indirectly to the performance of the MCP's obligations under the contract with DHCS. A network provider is not a subcontractor by virtue of the network provider agreement, as per 42 CFR § 438.2.
Waste	The overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare, Medicaid

TERMS	DEFINITION
	or any health care benefit program. Waste is generally not considered to be caused by criminally negligent actions.
Whistleblower	Someone who reports wrongdoing (by a co-worker, employer, or other person or company) to a person in a position of authority or publicly, such as to the media. More specifically, in a legal sense, it usually means someone who observes or learns of illegal activity, or at least activity believed to be unlawful, and reports it either to (1) a supervisor or other designated reporting recipient in the organization where the Whistleblower is employed or (2) to a governmental agency with responsibility to investigate or enforce laws regarding the alleged wrongdoing.

QUIZ

1. Allegations of fraud are limited to the intentional billing for services that do not meet professionally recognized standards.
    a. True
    b. False
2. What are some of the penalties for violating fraud and abuse (FA) laws?
    a. Fines
    b. Imprisonment
    c. Exclusion from participation in all health care programs
    d. All of the above
3. All of these government agencies except one are involved in fraud and abuse prevention, which one?
    a. CMS
    b. OIG
    c. LDR
    d. DMHC
4. What is/are cause(s) for improper payment?
    a. Upcoding
    b. Billing for services not needed or not rendered
    c. Misrepresentation of facts
    d. All of the above
5. Abuse may be intentional or unintentional: improper practice that either directly or indirectly results in unnecessary costs to health care program.
    a. True
    b. False
6. It is acceptable to obtain a verbal denial from the medical director without follow-up electronic or written signature.
    a. True
    b. False

7. It is always acceptable for a medical group to suppress availability of high-cost specialists in their system to encourage use of preferred providers.
    a. True
    b. False

8. The exclusion statute is a federal law which bans any provider or entity convicted of fraud from participating in any federally funded programs.
    a. True
    b. False

9. An example of Health Care fraud being an intentional act for gain is making prohibited referrals for certain designated services.
    a. True
    b. False
10. It is acceptable for a provider to receive cash or below-fair market value rent for a medical office space in exchange for referrals.
    a. True
    b. False
11. Which is NOT an example of Best Practices for Preventing Fraud and Abuse.
    a. Developing a compliance program
    b. Providing effective education of physicians, providers, suppliers, and members
    c. When encountering a potential violation of laws, regulations, policies, or contractual obligations, it is not our responsibility to report immediately
    d. Monitoring claims and medical records
12. When reporting Fraud, the group shall only report to their internal departments and regulators.
    a. True
    b. False
13. If economic profiling is practiced by the delegate, they must disclose to the plan and follow the economic profiling policy of the health plan or have their policy submitted to the DMHC for approval.
    a. True
    b. False
14. Red Flags are warnings or discrepancies that attract attention to potential fraud and abuse and do not require reporting until you have specific evidence of fraud and abuse.
    a. True
    b. False

15. When fraud is identified it must be reported internally and/or to affected Sponsors.
    a. True
    b. False
    c.
16. When preparing files for an audit, it is important to modify the dates on audit documents to ensure you are compliant with timeframes.
    a. True
    b. False
17. Once a corrective action plan (CAP) is started, the corrective actions must be monitored annually to ensure they are effective.
    a. True
    b. False
18. Ways to report potential Fraud and Abuse include:
    a. Telephone hotlines
    b. Mail drops
    c. In-person reporting to the compliance department / supervisor
    d. Special Investigations Units (SIUs)
    e. All of the above
19. Some of the laws governing health care fraud and abuse include the False Claims Act and the Anti-Kickback Statute.
    a. True
    b. False

RESOLUTION OF THE IMPERIAL COUNTY LOCAL HEALTH AUTHORITY AUTHORIZING WIRE TRANSFERS.

RESOLUTION NO._____

WHEREAS the Local Health Authority ("LHA") Commission is committed to the entity's autonomous operation as pursuant to section 8.03.070 of the Codified Ordinances of the County of Imperial and within section 14087.38 of the Welfare and Institutions Code.

WHEREAS, on November 13th 2023, the LHA Commission approved by majority vote the establishment of a Privacy Officer for the Local Health Authority to be assigned to the Senior Director of Compliance.

WHEREAS, to continue business operations in a timely manner the Imperial County local Health Authority is authorizing any of the below mentioned to complete these tasks.

NOW, THEREFORE, the LHA resolves as follows:

(1) The Recitals set forth above are true and correct and incorporated into this Resolution by this reference.

(2) The Privacy Officer's privilege is conveyed to those that hold the position of
   a. Chelsea Hardy, Senior Director of Compliance.

(3) The staff of LHA are hereby authorized and directed to take all actions necessary to carry out the intent and purpose of this Resolution.

(4) This Resolution shall take effect immediately upon its adoption.

PASSED AND ADOPTED by the Local Health Authority, County of Imperial, State of California, this _____day of _____ 2023, by the following roll call vote:

_____.

_____
Mr. Lee Hindman,
Chairman

ATTEST:

_____
Yvonne Bell
Vice-Chair

COMMUNITY HEALTH PLAN OF IMPERIAL VALLEY

To Apply email resume to contact@chpiv.org

Job Description: Senior Director of Compliance and Privacy Officer

Reports to: Chief Compliance Officer

POSITION SUMMARY

The Senior Director of Compliance and Privacy Officer has a key leadership role in the Compliance department and reports directly to the Chief Compliance Officer. The Senior Director of Compliance and Privacy Officer ensures the organization's adherence to state and federal regulatory requirements, as well as contractual obligations. This position leads a wide range of compliance functions and plays a critical role in maintaining CHPIV's commitment to compliance excellence and ethical practices.

The Senior Director of Compliance and Privacy Officer works closely with the CCO, collaborating on the development, implementation, and evaluation of the Compliance Program. The position will focus will be on establishing effective regulatory compliance functions including working with the Compliance management team in designing auditing and monitoring activities to prevent, detect, and correct any noncompliance issues promptly. The Senior Director of Compliance and Privacy Officer will oversee a dedicated team of compliance professionals, guiding and supporting them in their respective functions, including Regulatory Affairs, Regulatory Change Management, Audit Readiness, Regulatory Reports, ~~Privacy,~~ Fraud and Abuse Prevention, and Material Review.

As the CHPIV Privacy Officer, the Senior Director of Compliance and Privacy Officer is responsible for developing a HIPAA-compliant privacy program to ensure privacy policies are enforced to protect the integrity of protected health information (PHI). This position will oversee ongoing staff privacy training, conduct risk assessments, and develop HIPAA-compliant procedures where necessary and will monitor compliance with the privacy program, investigate incidents in which a breach of PHI may have occurred, report breaches to appropriate regulatory agencies as necessary, and ensure members´ privacy rights in accordance with state and federal laws.

The Senior Director of Compliance and Privacy Officer position is an at-will classification unless otherwise provided for in an employment contract.

ESSENTIAL DUTIES AND RESPONSIBILITIES

- Collaborate with the CCO to ensure Compliance ~~Program~~ and Privacy Program effectively prevents, detects, and corrects noncompliance issues and privacy incidents. Continuously assess and enhance the effectiveness of the Compliance and Privacy Program. Implement improvements based on audit findings, industry best practices, and regulatory changes.
- Analyze compliance standards and develop measures for assessing internal compliance. Generate valuable management reports and design specialized tools to identify potential compliance gaps and ensure prompt remediation. Provide regular status reports to the CCO, Leadership Team, and the Commission.

- Conduct comprehensive risk assessments to identify potential compliance risks within the organization. Develop and implement risk mitigation strategies to proactively address and minimize compliance-related vulnerabilities.
- Develop and deliver compliance training programs for employees, management, and relevant stakeholders. Promote a culture of compliance awareness and ethical conduct throughout the organization.
- Establish robust monitoring and auditing processes to proactively assess compliance with regulations, policies, and procedures. Regularly review internal controls and perform compliance audits to identify potential issues.
- Develop and maintain a policy management process for the organization that ensures annual reviews and updates. Develop, review, and update organizational policies, procedures, and forms to ensure regulatory compliance.
- Lead the design and implementation of a comprehensive regulatory change management process to ensure the organization remains informed about relevant regulatory changes and efficiently implements them.
- Serve as the primary point of contact with regulatory bodies such as the Department of Health Care Services and the Department of Managed Health Care. Address inquiries, requests, and reporting promptly and accurately.
- Conduct thorough investigations into reported compliance concerns and potential violations. Work closely with relevant departments and stakeholders to address and resolve noncompliance issues promptly and effectively.
- Travel Requirement: Travel within California as needed for compliance-related activities.

MINIMUM QUALIFICATIONS (KNOWLEDGE, SKILLS, AND ABILITIES, EXPERIENCE)

- Five years' experience in a licensed health care services plan, preferably a plan participating in the Medi-Cal managed care program.
- Five years' experience in operations including utilization management, provider credentialing, claims processing, quality improvement, fraud, waste, and abuse, HIPAA compliance, and preparing regulatory filings.
- Experience in health care service plans with significant delegation arrangements desirable Expert knowledge of compliance principles, laws, regulations, and industry best practices, with a proven track record of successfully implementing and maintaining effective compliance programs.
- Strong understanding of healthcare regulations, including but not limited to Medicare, Medicaid, HIPAA, and other relevant federal and state regulations governing managed care organizations.
- Comprehensive knowledge of auditing methodologies, risk assessment, and internal control frameworks to ensure thorough and accurate compliance assessments.
- Excellent leadership and people management skills, with the ability to lead, mentor, and inspire a diverse team of compliance professionals.
- Outstanding communication and presentation abilities, including the capability to articulate complex compliance issues in a clear and concise manner to various stakeholders, including executive leadership and regulatory authorities.
- High level of discretion and sound judgment when handling sensitive and confidential compliance matters.

- Able to work in a matrix organization with both the LHA and Delegate relationships.

IMPORTANT DETAILS

PHYSICAL DEMANDS AND WORK ENVIRONMENT

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this position. Reasonable accommodations may be made to enable individuals with disabilities to perform the functions. While performing the duties of this position, the employee is regularly required to talk or hear. The employee frequently is required to use hands or finger, handle, or feel objects, tools, or controls. The employee is occasionally required to stand; walk; sit; reach with hands and arms; climb or balance; and stoop, kneel, crouch, or crawl. The employee must occasionally lift and/or move up to 25 pounds. Specific vision abilities required by this position include close vision, distance vision, color vision, peripheral vision, and the ability to adjust focus. The noise level in the work environment is usually moderate.

NOTE

This job description in no way states or implies that these are the only duties to be performed by the employee(s) incumbent in this position. Employees will be required to follow any other job-related instructions and to perform any other job-related duties requested by any person authorized to give instructions or assignments. All duties and responsibilities are essential functions and requirements and are subject to possible modification to reasonably accommodate individuals with disabilities. To perform this job successfully, the incumbents will possess the skills, aptitudes, and abilities to perform each duty proficiently. Some requirements may exclude individuals who pose a direct threat or significant risk to the health or safety of themselves or others. The requirements listed in this document are the minimum levels of knowledge, skills, or abilities. This document does not create an employment contract, implied or otherwise, other than an "at will" relationship.