Compliance Program and Fraud, Waste, and Abuse Prevention

Compliance Program Overview

Community Health Center Network (CHCN) is a not-for-profit Medi-Cal managed care organization, providing business administrative support to community health centers providing health care to Medi-Cal beneficiaries, including but not limited to administering capitated health plan contract with The Alameda Alliance for Health (Alliance) for Medi-Cal enrollees and IHSS enrollees as well as maintains a large network of specialty providers.

CHCN is committed to preventing, detecting, and investigating Fraud, Waste, and Abuse (FWA) incidents to assure public accountability and conduct proper business practices. It is also the intent of CHCN to comply with federal and state regulations, and contractual requirements concerning the detection, investigation, and resolution of suspected fraud, waste, and abuse (FWA). The Compliance program will comply with Health & Safety Code § 1348 as adopted by the Department of Managed Health Care.

The purpose of CHCN Anti-Fraud Program is to:

- Protect CHCN's ability to deliver business administrative support services to the health centers through the timely detection, investigation, and prosecution of fraud.
- Develop and implement a process to protect CHCN from internal fraud and from external fraud by providers, employees, members, and others.
- Provide various methods to report potential fraudulent activities to the appropriate authorities at CHCN.
- Outline procedures for the detection, reporting, and managing of incidents of suspected fraud;
- Coordinate the practices and procedures for the detection, investigation, prevention, reporting, correcting, and prosecution of fraud with federal, state, and local regulatory agencies and law enforcement;
- Provide FWA awareness education and training to employees, members, and providers to facilitate in the timely detection and investigation of fraud, waste, or abuse; and
- Educate CHCN employees on applicable federal and state laws including the False Claims Act and whistleblower provisions.

Anti-Fraud Activities

The Anti-Fraud Program outlines the Compliance Department's areas of focus with regards to anti-fraud activities. The Anti-Fraud Program initiatives are compiled into seven main categories: Structure, FWA Reporting, Regulatory Reporting, Non-Retaliation, FWA Detection & Prevention, Investigation & Monitoring, and Education & Training.

Structure

The CHCN's Compliance Officer (CO) is responsible for the Compliance Anti-Fraud Program and activities. The CO reports directly to the Chief Executive Officer (CEO) with a dotted line to the Board of Directors. The CO chairs the Compliance Committee (Committee) which assists the CO in overseeing the Anti-Fraud activities. The CO is responsible for the daily operations of the program, and reports incidents and fraud prevention activity to the CEO weekly and the

Committee quarterly, or more frequently if needed. The CO reports to the Board of Directors on Compliance activities at the Board meetings.

The Committee is comprised of senior leadership roles from each operational area of CHCN. The Committee is responsible for reviewing and discussing CHCN monitoring activities, new or revised state and federal regulations related to fraud detection and prevention, and operational processes needed to comply with applicable regulations. The Committee reviews internal and external fraud investigation statistics conducted by the CHCN and discusses certain cases for resolution of any issues that arise. Any significant incidents are also reported immediately by the CO to the CEO, and will be reported to the Board of Directors by the CEO and/or CO.
CHCN's Compliance Department works closely with internal departments on fraud detection process and investigations. These departments include Utilization Management, Provider Services, Customer Care, and Claims. The Compliance Department collaborates with these departments to complete certain steps of the investigation process and to develop and monitor a corrective action plan. These steps may include provider and member outreach, medical utilization data analysis, clinical review of medical records, medical coder review, and monitoring of provider claims billing patterns.

Understanding FWA

1. Definitions of FWA:
   - Fraud: An intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to themselves or some other person.
   - Waste: The overutilization or inappropriate utilization of services and misuse of resources.
   - Abuse: Activities that are inconsistent with sound fiscal, business, or medical practices, and result in the following: unnecessary cost to health care programs or reimbursement for services that are not medically necessary or fail to meet professionally recognized standards for health care. Abuse also includes beneficiary practices that result in unnecessary costs to health care programs.

2. Examples of FWA
   The costs of fraudulent activities in public programs annually cost the state and federal taxpayers hundreds of billions of dollars. Below are examples of these types of activities:

   <u>Provider FWA</u>
   - Altering medical records to received covered services
   - Billing for services not provided or that are medically unnecessary
   - Services performed by an unlicensed provider yet billed under a licensed provider's name or information
   - Billing for non-covered services using incorrect CPT, HCPCS, and/or diagnosis code in order to have services covered
   - Payment for referrals including soliciting, offering, or receiving kickbacks or bribes
   - Unbundling of services that should be billed together and/or Upcoding
   - Balance billing Medi-Cal or Medicare beneficiaries for the difference between the allowed reimbursement rate and the customary charge for the service
   - Overutilization or underutilization

Member FWA

- Impersonation: Someone using the personal information of another person to obtain Medi-Cal or Medicare benefits for which they would otherwise not qualify or be entitled to receive
- Relocating to out-of-service area for which their benefits are assigned
- Falsely reporting of money or resources in order to obtain benefits
- Providing inaccurate or incomplete information about a medical condition to get medical treatment
- Forging, altering or selling prescriptions
- Obtaining controlled substances from multiple providers
- Using more than a single provider to obtain similar treatments and/or medications

FWA Reporting

CHCN requires employees, contracted network providers, and members to report any potential FWA incidents for investigation as soon as it is known. To assist us in our investigation efforts, please include as much of the following information as possible when reporting a potential FWA incident:

- Name, address, license number, or insurance ID of the suspect (if known)
- Description and details of the incident including who, what, where, and when with the date and time of the incident(s)
- Any documentation you have related to the incident(s)
- Your name and telephone number (if you would like to be contacted)

Individuals may report potential FWA incidents using any of the following methods:

- Contacting CHCN's Compliance Officer, Teresa Ercole directly by:
  - Phone: (510) 297-0290
  - Email: tercole@chcnetwork.org
- Or via email to our Compliance Department at compliancemailbox@chcnetwork.org
- Or calling our Toll-Free Hotline week at (833) 222-1507
  - The Compliance Hotline is a live twenty-four hours a day telephone line that can be accessed by anyone who would like to report concerns or alleged violations. Providers, members, employees, and any others can report anonymously through the hotline.

Reporting to the Appropriate Regulatory Agencies and Plans

CHCN's Compliance Department independently reports to the Department of Managed Health Care (DMHC) and Department of Health Care Services (DHCS) when appropriate to coordinate FWA investigations with the regulatory agencies. It also independently reports to the Alliance when appropriate and coordinates with them to conduct FWA investigations involving their enrollees or networks. CHCN's Compliance Department also provides documentation as requested to the appropriate state and federal law enforcement agencies. Based on the preliminary investigation, if there is reason to believe a fraudulent activity occurred with respect

to a Medi-Cal enrollee, CHCN will immediately report the incident to the Alliance. CHCN will follow up on the incident and provide the Alliance with all investigation case documentation as necessary.

Non-Retaliation Policy

It is the policy of CHCN that no person shall be retaliated or discriminated against for reporting in good faith to any of the reporting methods listed above or to other proper authorities any alleged fraudulent activity committed by, on behalf of, or against CHCN.

The False Claims Act (FCA) also contains Qui Tam or "whistleblower" provisions. A "whistleblower" is an individual who reports in good faith an act of fraud, waste, and abuse to the government, or files a lawsuit on behalf of the government. Whistleblowers are protected from retaliation from their employer under Qui Tam provisions in the FCA and may be entitled to a percentage of the funds recovered by the government.

FWA Detection & Prevention

CHCN strives to detect and prevent health care fraud, waste, and abuse. A variety of oversight mechanisms are used to detect fraud by employees, providers, vendors, and members. The three core drivers for detecting fraud are claims fraud data detection, fraud/suspicious reporting, and provider suspension/exclusion screening.

1. Fraud Data Detection

   Provider claims data is routinely analyzed by the Claims Department in conjunction with the Compliance Department to detect any fraudulent activity. Data analyzed is specific to providers, facilities, members, and medical services. When suspected claims are identified, the suspected claims are reviewed to determine if further investigation is valid and necessary, and if valid will proceed with additional investigation which may include medical records review, claims history review, and billed code analysis. This data analysis is critical for monitoring and identifying any repetitive fraud, waste, and abuse patterns, such as for example, over/under utilization, false claims. Unusual billing practices are also measures reviewed in the data analysis. Analysis findings are reported to the CO and, if warranted, to the Compliance Committee, CEO and Board of Directors.

2. Fraud/Suspicious Reporting

   The identification and prevention of fraud, waste, and abuse is a cooperative effort that includes all employees, providers, and members reporting any suspicious activities or claims to CHCN for investigation. The Compliance Department tracks and trends fraudulent cases reported to identify patterns with specific claims billed services, provider types, provider facilities, and medical services and durable medical equipment. From the reporting trends found, the Compliance Department will work closely with the Claims, Provider Network Management, and Quality Management Departments to monitor and investigate the trends closely to determine if there are any root causes for the specific high volume FWA cases.

3. Provider Suspensions/Exclusion Screening

   CHCN conducts monthly exclusion screening of all providers of health care services, as well as prior to contracting, to verify whether they have not been the subject of adverse government actions related to fraud, patient abuse, licensing board sanctions, license revocations, suspensions, and/or excluded from participation with the Office of Inspector General (OIG), System for Award Management (SAM), and Medi-Cal health care programs.

Investigation & Monitoring Procedures

All reported potential fraud, waste, or abuse incidents are reviewed and prioritized for investigation. The intent of the FWA investigation is to find and correct actions that lead to fraudulent or wasteful payments, overpayment recoveries related to fraudulent or wasteful activities, and work in collaboration with regulatory authorities and law enforcement. The investigator will conduct desktop reviews of the relevant documentation and data requested to conduct the investigation.

In some cases, it will be necessary to visit the site of the potential fraud (i.e. provider's office or vendor site) to guarantee the integrity of the documentation. The quality and credibility of the allegations will also be assessed along with the review of the questionable documentation to determine if fraudulent.

Corrective action plans and follow-up investigation plans are included, if applicable, to ensure any open issues and deficiencies are corrected. Corrective action plans may include the following actions: medical record review, claims audit, provider education, provider claims monitoring, overpayment recoveries, and termination. Findings are reported to the CO and to the Compliance Committee.

Education & Training

All CHCN employees are required to complete the Fraud, Waste, and Abuse Compliance training upon hire and annually thereafter. The comprehensive FWA training provides a basic understanding of how to detect fraud, waste and abuse, and why it is important to report any suspicious activity.

The training covers, among other topics, the following key concepts:

1. What is fraud, waste, and abuse;
2. How to detect and prevent FWA;
3. Warning signs for common FWA problems and examples;
4. FWA applicable statutes and laws;
5. Legal consequences and costs of FWA;
6. How to report potential FWA; and
7. Non-retaliation against reporting.

Disciplinary standards will be enforced to employees that do not meet the FWA training requirements.

Providers receive FWA education and training materials through the CHCN Provider Manual. The CHCN Provider Manual provides an overview of the importance of FWA detection, reporting, and prevention. The methods of reporting incidents and CHCN's Compliance Department contact information are included in the online FWA materials.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a federal law that requires the CHCN and its network providers to protect and maintain the security and confidentiality of its members' Protected Health Information (PHI) and to provide its members with certain privacy rights. PHI is any individually identifiable health information, including demographic information. PHI includes but is not limited to the member's name, address, phone number, medical information, social security number, ID card number, date of birth, and other types of personal information. This section of the Provider Manual seeks to guide network providers on the following: 1) implementation of safeguards to protect CHCN member PHI; 2) ensure appropriate uses and disclosures of PHI; 3) ensure members can timely access their own PHI; and 4) how to identify and report privacy incidents and breaches to the CHCN.

Safeguarding PHI

As covered entities under the HIPAA Privacy Rule, CHCN, and its network providers must comply with HIPAA requirements. Below are a few reminders on how to protect and secure PHI.

- Documents containing PHI should not be visible or accessible to visitors or others who are unauthorized to have access to PHI.
- When faxing documents containing PHI, verify the recipient, the recipient's fax number, and the documents being sent.
- Ensure that outgoing faxes include a fax cover sheet that contains a confidentiality statement.
- When mailing PHI, verify the recipient, the recipient's mailing address, and the documents being sent.
- Ensure that envelopes and packages are properly sealed, secured, and if using a clear window envelope, ensure that information is not visible through the window of the envelope, prior to mailing out.
- When transporting PHI, ensure that the information is protected by using binders, folders, or protective covers.
- PHI must not be left unattended in vehicles.
- PHI must not be left unattended in baggage at any time during traveling.
- PHI should be locked away during non-business hours.
- PHI must be properly disposed of by shredding. Never recycle or dispose of documents containing PHI in the trash bin.

PHI IN ELECTRONIC FORM

- When transmitting PHI via email ensure that the email is encrypted. This prevents anyone other than the intended receiver from obtaining access to the PHI.
- Do not include PHI such as an individual's name or beneficiary ID number (CIN) in the subject line of the email.
- Confirm the recipient, recipient's email address, and documents or information being sent, prior to sending the email.

- Ensure all portable data storage devices (CDs, DVDs, USB drives, portable hard drives, laptops, etc.) are encrypted.

PHI IN ORAL FORM

- Do not discuss PHI in public areas such as the patient waiting room.
- Do not discuss PHI with unauthorized people.
- Always verify the identification of an individual prior to discussing PHI with the individual.
- Ensure to speak quietly when discussing PHI.

Uses and Disclosures of Member PHI

The HIPAA Privacy Rule allows member PHI to be used and disclosed without the member's written consent for the following reasons (not a complete list):

- Treatment
- Payment
- Health care operations
- Court and administrative proceedings
- Health oversight activities
- Public health activities
- Law enforcement purposes

Network providers must obtain specific written consent through a HIPAA Compliant Authorization Form for all other uses and disclosures of PHI not for treatment, payment, or health care operations or otherwise permitted or required by the HIPAA Privacy Rule.

Member Access to PHI

The HIPAA Privacy Rule requires the CHCN and its network providers to provide members, upon request, with access to their PHI. Providers must ensure that their medical records systems allow for prompt retrieval of medical records and that these records are available for review whenever a member requests access to their PHI. Providers must also provide the member with timely access to their PHI in the form and format requested by the member.

Reporting of Privacy Incidents and Breaches to the CHCN

The HIPAA Privacy Rule requires covered entities to provide notification to enrollees following a breach of PHI. Network Providers must immediately and upon discovery report both privacy incidents and breaches involving CHCN members. A privacy incident is defined as an event or situation where an individual or organization has suspicion or reason to believe that PHI may have been compromised. Privacy incidents include but are not limited to the following:

- PHI sent to the wrong individual or organization.
- PHI sent unencrypted.
- Loss or theft of documents containing PHI in paper or electronic form.
- Loss or theft of unencrypted devices (laptop, hard drives, USB drives).
- Loss of access or other threat to network servers containing PHI.

A breach is defined as unauthorized access, use, or disclosure of PHI that violates either federal or state laws, or PHI that is reasonably believed to have been acquired by an unauthorized person. Timely reporting of incidents and breaches involving the PHI of our members is crucial in the response, investigation, and mitigation of incidents and breaches.

To report suspected or known privacy incidents and breaches you may contact the CHCN Compliance Department through any of the following means:

- Contacting CHCN's Compliance Officer, Teresa Ercole directly by:
  - Phone: (510) 297-0290
  - Email: tercole@chcnetwork.org
- Or via email to our Compliance Department at compliancemailbox@chcnetwork.org
- Or calling our Toll-Free Hotline at (833) 222-1507
  - The Compliance Hotline is a live twenty-four hours a day telephone line that can be accessed by anyone who would like to report concerns or alleged violations. Providers, members, employees, and any others can report anonymously through the hotline.