

CHILDREN FIRST MEDICAL GROUP



General Compliance Training 2025



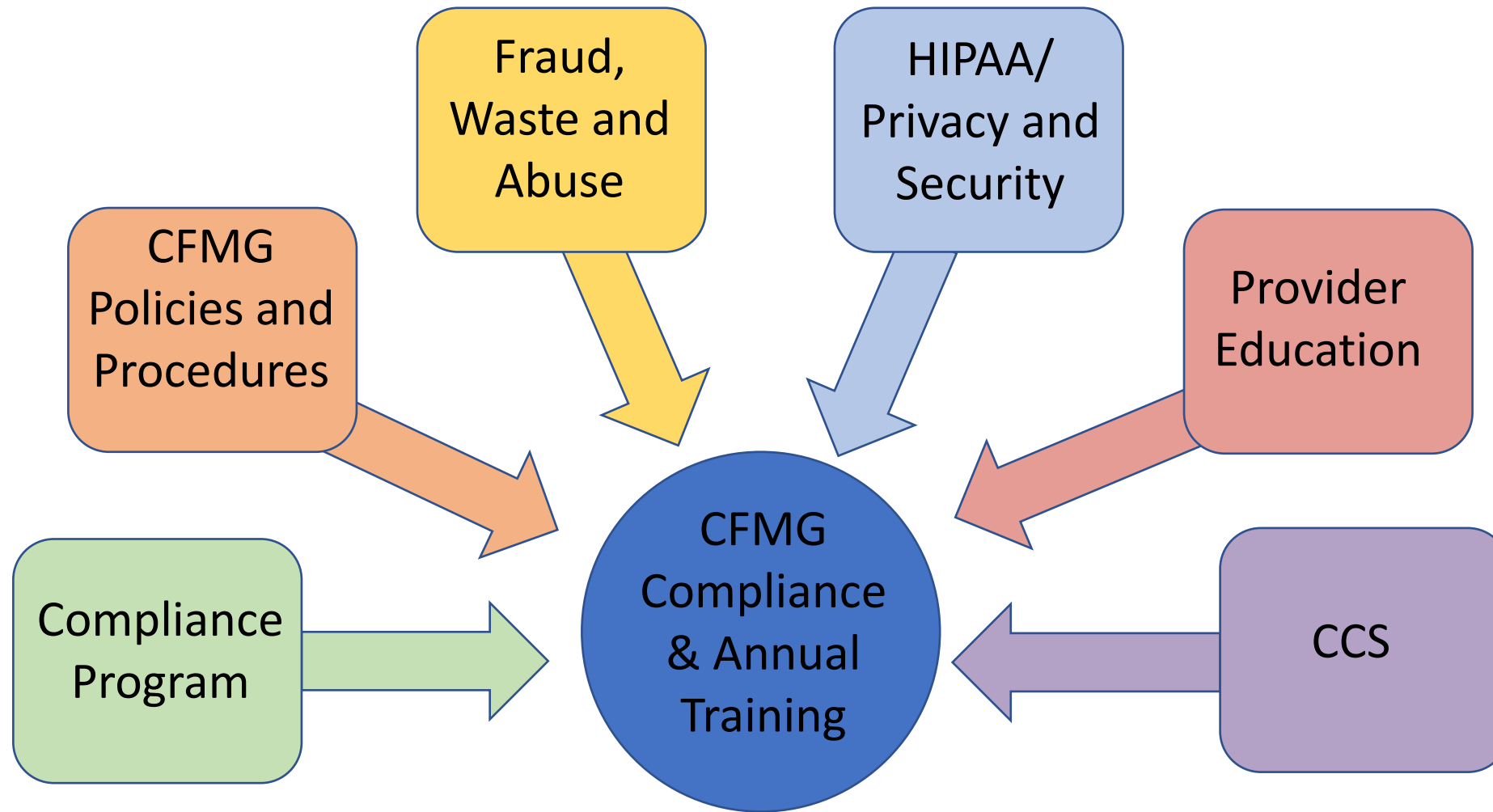
Table of Contents/Agenda



Objectives:

- Understand why you need Compliance Training and how Compliance effects everyone
- Learn about the 7 elements of an effective Compliance Program
- Learn about OIG/SAM/Medi-Cal exclusions list
- Learn about Fraud, Waste and Abuse
- Learn about HIPAA/Privacy & Security
- Learn about Provider Education
- Learn about CCS

Compliance Training: Overview



Compliance Training: Overview

Annual Compliance Training is mandatory for:

- Team Members
- Temporary Staff
- Contractors
- Consultants
- Interns
- Business Associates
- Governing Boards
- Chief Officers

Introductory Compliance Training

- First Tier entities including IPAs (CFMG) must ensure Introductory Compliance training is provided to all required individuals and entities within 90 days of hire or start.
- CFMG must provide Compliance training to their staff and attest on an annual basis that training has been provided to all employees.

FDR - Definition

- **F** – First Tier Entity: IPA, Hospital, Benefit Manager, pharmacy, (PBM)
- **D** – Downstream Entity: (e.g., Pharmacy contracted with PBM, claims processing contracted with IPA)
- **R** – Related Entity: (e.g. common ownership or control entity)

What is Compliance and Why is it important?

Federal and State laws regulate the Health Care Industry

To ensure
compliance with
applicable laws

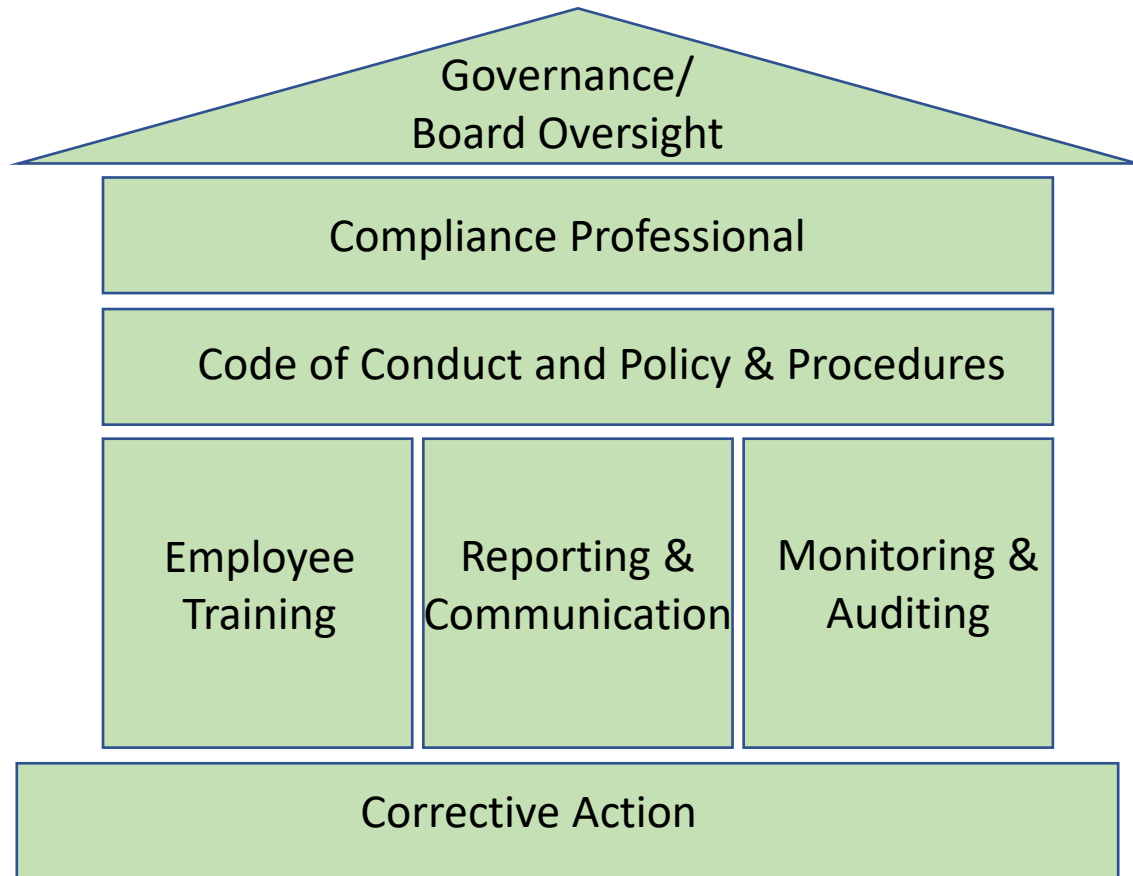
To protect our
members

To prevent abuse
of Federal and
State taxpayer
money

To guide CFMG to
always to do the
right thing!

Corporate Compliance Program Structure OIG Guidance: 7 elements

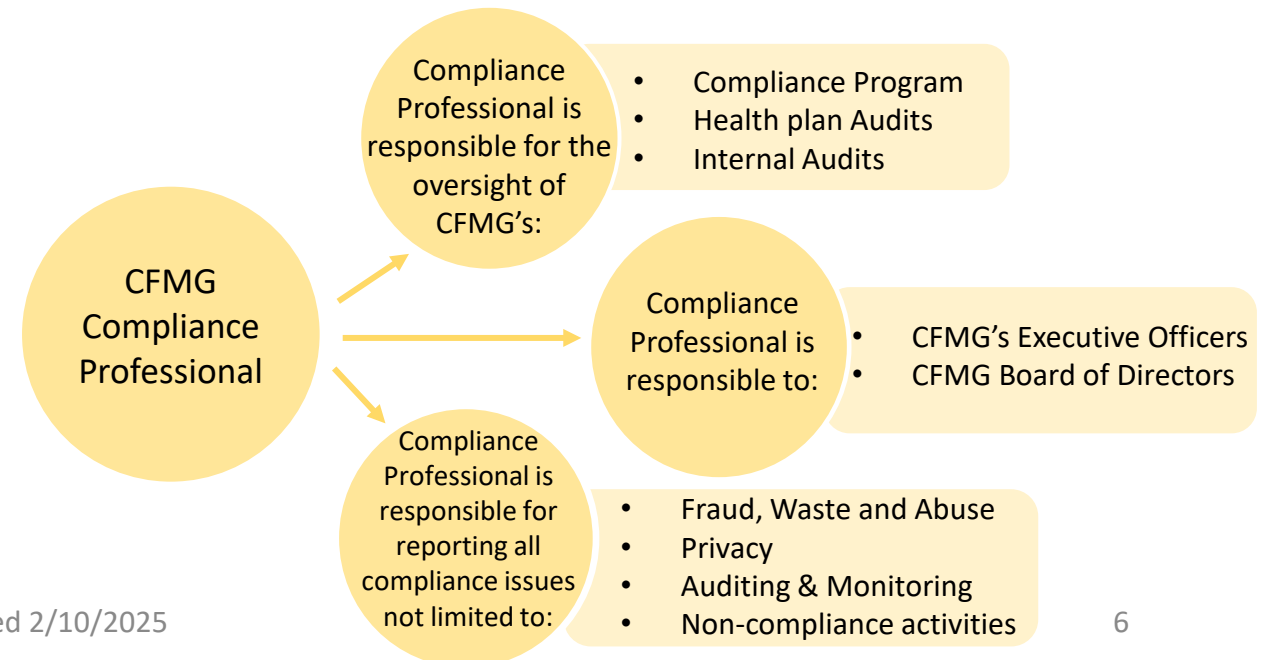
The Federal Sentencing (FSG) and Office of the Inspector General (OIG) have identified 7 elements of an effective Compliance Program:



Element 1: Written Policies, Procedures and Standards of Conduct

- ❖ Ensure all team members are familiar with CFMG P&Ps
- ❖ Show commitment to comply with Federal and State standards
- ❖ Provide Guidance to Team Members, Business Associates, Vendors and FDRs with issues related to Fraud, Waste and Abuse, HIPAA Privacy & Security, and other issues of non-compliance.
- ❖ Identify how to communicate compliance issues

Element 2: Compliance Professional and High-Level Oversight



Corporate Compliance Program Structure OIG Guidance: 7 elements

The Federal Sentencing (FSG) and Office of the Inspector General (OIG) have identified 7 elements of an effective Compliance Program:

Element 3: Effective Training and Education

CFMG must be able to demonstrate that their employees have fulfilled these training requirements. Examples of proof of training may include copies of sign-in sheets and electronic certifications from the employees taking and completing the training.

Element 4: Effective Lines of Communication

CFMG must establish effective lines of communication, ensuring confidentiality between the compliance professional, members of the compliance committee, CFMG employees, managers and governing bodies. Such lines of communication must be accessible to all and allow compliance issues to be reported, to include a method of anonymous reporting.

Element 5: Corrective Action

CFMG is committed to conducting its operations in compliance with all applicable laws, regulations, and rules. As a part of this commitment, CFMG conducts regulatory sanction and exclusion screening of employees, temporary employees, consultants, volunteers, governing body members prior to start date and monthly thereafter to ensure that none of these persons or entities are excluded or become excluded from participation in Federal or State Programs. This sanction screening includes validating the Office of the Inspector General (OIG), System of Award Management (SAM) and the Medi-Cal Suspended and Ineligible List.

Element 6: Monitoring, Auditing, and Identification of Compliance Risks

- ❖ Internal monitoring activities are regular reviews that confirm ongoing compliance and ensure that corrective actions are undertaken.
- ❖ Internal Auditing is a formal review of compliance with a particular set of standard procedures that are used as a base measure.

Element 7: Prompt Responses to Compliance Issues

- ❖ Compliance will review and report on a quarterly basis any compliance issues to the Board.
- ❖ Compliance will notify the proper regulatory agencies when needed

Fraud, Waste and Abuse: Detection, Prevention and Correction

What is Fraud?

- The intentional (knowing and willful intent) misrepresentation of data or facts for financial gain. It occurs when a person knows or should know that something is false and knowingly deceives someone for monetary gain.

Some examples are:

- Billing for services not furnished or provided
- Soliciting, offering, or receiving a kickback, bribe or rebates
- Offering beneficiaries, a cash payment or other incentives to enroll in the plan
- Intentionally and repeatedly billing at a higher rate, or unbundling claims
- Collecting higher co-pays than specified
- Using someone else's Member ID to receive services
- Medical identity theft
- Eligibility (member state they live in a service area; misstatement of income)
- Drug seeking behavior (Doctor shopping; selling medications)
- Billing for prescriptions that are never picked up
- Additional dispensing fees for split prescriptions when the entire prescription cannot be filled



Fraud, Waste and Abuse: Detection, Prevention and Correction



What is Waste?

- The overutilization of services that results in unnecessary costs. Waste is generally not considered to be caused by criminally negligent actions but rather a misuse of resources.
- It is the extravagant, careless or needless expenditure of healthcare benefits and/or services, which results in unnecessary costs. Waste is considered a misuse of resources.

Some examples are:

- Providing medically unnecessary services, such as additional tests or procedures; and
- Failure to provide medically necessary services
- Performing unnecessary services for a member

Fraud, Waste and Abuse: Detection, Prevention and Correction



!!!Suspected Fraud, Waste and Abuse incidents must be reported immediately or at maximum within 24 hours of incident. Email: Catalina.Valderrama@ucsf.edu!!!

What is Abuse:

- Includes actions that may, directly or indirectly, result in unnecessary costs, improper payment, payment for services that fail to meet professionally recognized standards of care, or services that are medically unnecessary.
- Abuse involves payment for items or services when there is no legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment

Some examples are:

- Re-ordering the same lab tests because the report could not be found in the chart
- Providing services that do not meet professionally recognized standards
- Inadvertently and consistently using the incorrect billing code on a claim
- Failure to effect timely disenrollment of a beneficiary from systems
- Hospital billing issues, e.g. incorrect billing practices
- Overprescribing narcotics

Federal Healthcare Fraud Laws

False Claims Act (FCA)

California:

- Recovered hundreds of millions of dollars
- Liable for up to three times the amount of money fraudulently obtained
- Whistleblower protection

Federal

- Imposes liability on individuals or entities who defraud governmental programs
- Whistleblower protection
- 2014: 89% of all False Claim actions were initiated by whistleblowers
- 2014: 5.7 billion dollars recovered

Anti-Kickback Statute

- Knowingly or willfully soliciting, receiving, offering or paying for referrals for services (e.g. kickback, bribe, or rebate)
- Violations are punishable by a fine of up to \$25,000; imprisonment for up to 5 years; or both.

Stark Statute Damages and Penalties

- Prohibits a physician from referring patients for designated health services to an entity with which the physician (or member of his or her family) has a financial relationship, unless an exception applies
- Prohibits the designated health services entity from submitting claims for those services resulting from a prohibited referral
- A penalty of up to \$15,000 may be imposed for each service provided; may also be up to a \$100,000 fine for entering into an unlawful arrangement

Civil Monetary Penalty:
Penalty range from \$5,000 and \$11,000 for each false claim and damages may be tripled.

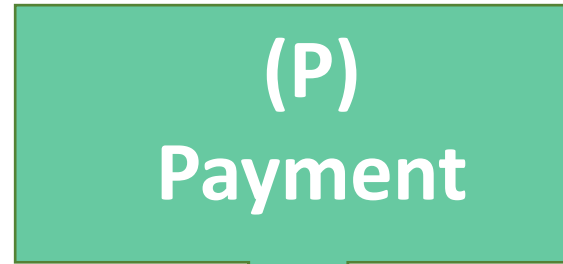
!!!Suspected Fraud, Waste and Abuse incidents must be reported immediately or at maximum within 24 hours of incident. Email: Catalina.Valderrama@ucsf.edu!!!

Treatment, Payment and Operations

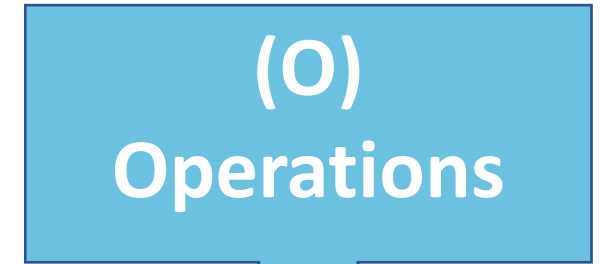
The law only allows disclosure of PHI under the following categories:



When the information requested is needed to treat our members



When the information is needed to provide payment for services that a Member received



When the information is used for health care operations

HIPAA/Privacy Security

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Creates greater access to health care insurance, protection of privacy of health care data, and promotes standardization and efficiency in the health care industry.

Provides safeguards to prevent unauthorized access, use, or disclosure of protected health care information.

As an entity who has access to protected health care information of our members, you are responsible for complying with the HIPAA guidelines.

Violations may result in civil monetary penalties. In some cases criminal penalties may apply.

Suspected HIPAA incidents must be reported immediately or at maximum within 24 hours of incident. Email: Catalina.Valderrama@ucsf.edu



HIPAA/Privacy Security/HITECH

- Requires that healthcare entities take specific steps to ensure that member protected health care information (PHI) is not viewed by anyone without “a business need to know,” is not stolen, lost or accidentally destroyed.
- Requires that Members be provided with rights over the use and disclosure of their own PHI
- HIPAA/HITECH Safeguards information that is stored or transmitted electronically such as ePHI. The Act was created to motivate the implementation of electronic health records (EHR).
- HIPAA Privacy Rule covers certain health information in any form.

Protected Health Information (PHI)

- Individually identifiable health information that relates to a Member’s past, present, or future physical or mental health or condition, including the provision of his/her health care, or payment for that care (such as claims, enrollment and disenrollment)
- A breach of PHI means the impermissible access, use or disclosure of PHI which compromises the security or privacy of the PHI

Personally Identifiable Information (PII)

- Information that either identifies the Member or there is a reasonable basis to believe that the information can be used to identify the Member, such as name, date of birth, address, or Social Security Number. Other personal identifiers include, but are not limited to, CFMG ID numbers, Medi-Cal ID numbers, phone numbers, e-mail addresses, photographic images, financial information, such as transaction receipts, bank account or credit card numbers.

Minimum Necessary

- All reasonable efforts should be made to access, use, disclose and request only the minimum amount of PHI needed to accomplish the intended purpose of the access, use, disclosure or request.

Common PHI Breaches



Unauthorized access

Looking into
Family/Friends Accounts

Viewing Member
information without a
“business need to know”-
Misdirected documents

Sending documents to an
incorrect fax number –
Always confirm the fax
number

Mailing/handing
documents by mistake to
the wrong Member -
Always Double Check

**-Unauthorized verbal
disclosure**

Phone

Voicemail

In person – Use
discretion near others
who are in proximity and
may overhear

Lost, missing or stolen
mobile devices that
contain unencrypted data

Phones, laptops, tablets

Improper disposal of
documentation,
computers or other
material (e.g. throwing
PHI in regular trash bin)

Unsecured E-Mail
containing Member
information

Web access creating data
security risks (social
media)

Privacy Training Tips

Discuss	Never discuss PHI where you may be overheard
Access	Access member PHI only when it pertains to your job
Use	Use the designated shredder bin to destroy PHI
Confirm	Confirm phone number and fax numbers prior to use
Confirm	Confirm you are speaking with the member or authorized representative before discussing PHI by requesting multiple patient identifiers to authenticate the individual you are speaking with
Lock	Lock your computer when leaving your work area and lock any PHI in your drawers



Security Training Tips

- Assure that office staff use a secure method for sending SECURE e-mails. Related to any external electronic transmittal of ePHI
- Assure that the office server is in a secure area
- Paper based PHI should always be kept in a secure area
- Change your password/s often
- Do not leave your password/log-in information in or around the office area
- Password sharing is prohibited
- When walking away from your desk always lock your computer: Ctrl+Alt+Delete and turn any documents containing PHI facedown
- When leaving for the day, lock your workstation and any drawer that contains PHI, make sure all paper documents containing PHI are placed in the designated shredder bin

Privacy Training Tips for the General Medical Setting



Every staff member in the office should be appraised of HIPAA standards and held accountable



Do not discuss sensitive issues when the patient is standing in the reception window and within earshot of those in the waiting room



Use a patient sign-in system that allows the reception staff to remove or obstruct the name after sign-in



When retrieving a patient from the waiting room for their appointment, use only their first name



When placing charts for the physician, position in such a way that the patient names are not visible



Offices should have a partition system/window so that those in the waiting area cannot hear business conducted by staff members



When leaving appointment reminder phone calls to patient, exercise caution to leave PHI in your message



Always err on the side of caution



Chapter 21 50.7.1

When serious noncompliance or waste occurs, you are strongly encouraged to refer the matter to CMS.

Reporting Fraud, Waste and Abuse

- *Every Team Member has the right and responsibility to report suspected Fraud, Waste and Abuse and any other suspected Compliance Violations.
- *Not reporting fraud or suspected fraud can make you a part of a case by allowing it to continue.
- *You may report anonymously 24 hours a day.
- *Suspected HIPAA incidences must be reported within 24 hours
- *Retaliations are *prohibited* when you report a concern in good faith.

Consequences of Non-Compliance

- *Staff that fails to report potential Fraud, Waste & Abuse or other Compliance violations in a timely manner will be subject to disciplinary action up to and including summary termination.
- *Noncompliance or Fraud, Waste, & Abuse committed by employee will be logged and a corrective action plan will be put in place if appropriate. Should the corrective action plan not be implemented by the employee, it will result in further disciplinary actions and/or leading up to termination.

Ways to Report Compliance Concerns or for Compliance Questions

Reporting Suspected or detected non-compliance, FWA or Privacy Issues is your responsibility.

Ways to report:

*Alameda Alliance for Health 855-747-2234
*Medi-Cal 800-822-6222
*Centers for Medicare & Medicaid Service 800-477-8477
*NBI Medic (pharmacy) 877-7SA-FERX
*CFMG 510-428-3885 ext. 4259 or
email: Catalina.Valderrama@ucsf.edu

- Reports can be anonymously
- Report Suspected Fraud, Waste and Abuse
- Report Suspected Privacy Issues/HIPAA Issues within 24 hours
- Reporting is available 24hours/7 days a week
- CFMG has a non-retaliation policy.




California Children's Services (CCS)

- Members, ages 0-21 can receive care through California Children Services (CCS) for specific medically eligible conditions (see below). CCS financial eligibility is automatic with their Medi-Cal coverage.
- Providers who know that the member has a CCS-eligible condition and/or an open case should obtain authorization for services for that condition directly from CCS. CFMG will also refer cases, obtain authorization, and forward claims for payment based on diagnosis or when an open case exists.
- If the condition is not CCS medically eligible or if CCS eligibility is uncertain, providers should follow the CFMG authorization procedures.
- CFMG Utilization Management staff will notify Health Plans of CCS referrals monthly per contractual agreement.

Coordination of Care

- Children with CCS-eligible conditions should still see their PCP for routine care, urgent care of non-eligible conditions, and for preventive care, including immunizations.
- CFMG relies on PCPs to coordinate services with CCS specialty providers. If the member is eligible for CCS services, CCS will provide medical case management for the specific CCS condition. In all cases, PCPs must continue to provide primary case management to the member.



Information for
Language/interpreter
services for Alameda
Alliance for Health is
available on the CFMG
website, under the
“Compliance” section

CFMG & Provider Education

CFMG provides annual education to CFMG providers, including the Health Plan’s Language Assistance Program (LAP) materials. The Group will educate contracted providers, provider staff, and Medical Group staff regarding their responsibilities through Provider Workshops, CFMG website, Provider Manual, reference guides, and newsletters. The Group also provides ongoing in-services by Contracting and Provider Relations staff as needed.

For additional resources or more information please see below.

Privacy:

- U.S. Department of Health and Human Services: refer to HIPAA for Professionals [HIPAA for Professionals | HHS.gov](#)
- California Department of Health Care Services: refer to FORMS, LAWS & PUBLICATIONS – PRIVACY & HIPAA [Data Privacy](#)
- Department of Health Care Services Medi-Cal: refer to References Tab – HIPAA [References Page](#)

Federal and State Sanction and Exclusions Lists

- Office of Inspector General List of Excluded Individuals: https://oig.hhs.gov/exclusions/exclusions_list.asp
- General Services Administrator System for Award Management: www.sam.gov
- California Department of Health Care Services Medi-Cal Suspended and Ineligible Provider List: [Provider Suspended and Ineligible List \(S&I List\) - Dataset - California Health and Human Services Open Data Portal](#)

General Compliance Program

- Office of Inspector General Measuring Compliance Program Effectiveness Resource Guide [Compliance Toolkits | Office of Inspector General | Government Oversight | U.S. Department of Health and Human Services](#)
- Centers for Medicare & Medicaid Services Provider Compliance Resources: <http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/ProviderCompliance.html>

Available Resources

Thank you for participating and expanding compliance program effectiveness by ensuring you and your organization incorporate the information into your daily operations and business practices.

If you have any Compliance questions, please email Catalina Valderrama at Catalina.Valderrama@ucsf.edu

Thank you