ALAMEDA Alliance FOR HEALTH

Health care you can count on.
Service you can trust.

Compliance Plan

APPROVED: 5/20/2025

Contents

INTRODUCTION

The Alameda Alliance for Health (Alliance) is committed to conducting its business operations in compliance with ethical standards, contractual obligations, and all applicable state and federal statutes, regulations, policies, in all products and services involved in the oversight and operations of health plans. The Alliance's commitment to ethical standards and conduct applicable to its own internal business operations is extended to business partners and providers through its oversight and monitoring responsibilities. The Compliance Program applies to all Alliance lines of business.

The comprehensive Compliance Program described here incorporates the fundamental elements of an effective compliance program that meets the regulatory requirements set forth at 42 C.F.R. §§422.503(b)(4)(vi) and 423.504(b)(4)(vi), which are reflected in the guidelines set forth by the Centers for Medicare and Medicaid Services (CMS) via Chapter 9 of the Prescription Drug Benefit Manual, and Chapter 21 of the Medicare Managed Care Manual, as well as identified by the U. S. Department of Health and Human Services' Office of Inspector General (OIG).The following are ways the Alliance Compliance Program addresses the Seven Elements of an Effective Compliance Program:

1. **Written Policies, Procedures, and Standards of Conduct**

    - The Alliance will develop, implement, and maintain written compliance policies, procedures, and standards of conduct.
    - These documents will articulate the company's commitment to comply with all applicable federal, state, and contractual requirements.
    - The Code of Conduct will be distributed to all employees, contractors, and relevant business partners.

2. **Compliance Program Oversight**

    - A Compliance Officer will be appointed to oversee the compliance program.
    - A Compliance Committee will be established to assist the Compliance Officer.
    - The Compliance Officer will report directly to the CEO and the Board of Directors.

3. **Training and Education**

    - All employees will receive compliance training upon hiring and annually thereafter.
    - Additional role-specific training will be provided, as necessary.
    - Training will cover federal and state regulations, company policies, and the Code of Conduct.

4. **Effective Lines of Communication**

    - Multiple channels for reporting compliance concerns will be established, including an anonymous hotline.
    - A non-retaliation policy will be strictly enforced to protect those who report concerns in good faith.
    - The Compliance Officer will maintain an open-door policy for discussing compliance issues.

5. Internal Monitoring and Auditing

- The Alliance has a formal Audit and Monitoring Plan, updated annually. This plan is subject to change throughout the year as risks change.
- Regular audits and risk assessments will be conducted to identify potential compliance risks.
- Monitoring activities will focus on high-risk areas specific to managed care operations, as identified during the Annual Risk Assessment.
- Results of audits and monitoring activities will be reported to senior management and the Board.

6. Enforcement of Standards

- Disciplinary policies will be consistently enforced for compliance violations.
- Disciplinary actions will be clearly communicated and applied fairly across all levels of the organization.
- Employment or contractor agreements will include compliance obligations.

7. Prompt Response to Detected Offenses

- A system for timely investigation of reported compliance issues will be maintained.
- Corrective action plans will be developed and implemented, as necessary.
- Self-disclosure protocols will be followed for reporting violations to appropriate authorities when required.

The Compliance Program is continually evolving and will be modified and enhanced based on compliance monitoring and identification of areas of business or legal risk.

For purposes of this Compliance Plan, unless otherwise defined, a reference to "employee or employees," made hereafter, means a "governor, employee, staff, trainee, vendor, contractor or sub-contractor" of the Alliance.

THE COMPLIANCE PROGRAM

This document addresses the fundamental elements of a compliance program. The Compliance Program establishes the Alliance principles, standards, and Policies and Procedures regarding compliance with applicable laws and regulations, including those governing relationships among the Alliance and federal and state regulatory agencies, participating providers, and Employees. The Compliance Program is designed to ensure accountability throughout the organization, the Alliance's operations and that the practices of all Employees comply with applicable contractual requirements, ethical standards, laws, and regulations. The Compliance Program relies on the greater coordination of Alliance Employees to ensure rules are followed across the organization.

The Compliance Program was initially approved by the Alliance Chief Executive Officer (CEO) and the Alliance Board of Governors (Board) and is reviewed annually by Compliance Committee and every two years by the Compliance Advisory Committee and Board of Governors.

Key Elements of the Alliance Compliance Program

I. Standards of Conduct, Policies and Procedures: The Compliance Program outlines how contractual and legal standards are reviewed, communicated, and implemented throughout the organization. New and modified standards are reviewed on a regular basis to develop Policies and Procedures and implement plans to meet contractual and legal obligations.

II. Oversight: The successful implementation of the Compliance Program requires dedicated commitment and diligent oversight throughout the Alliance's operations, including, but not limited to, key roles and responsibilities by the Board, Chief Executive Officer (CEO), Chief Compliance Officer (CCO), Compliance Advisory Committee, Compliance Committee, Delegation Oversight Committee and Executive Staff.

III. Effective Training and Education: The Alliance requires that all Employees complete training upon appointment, hire, or commencement of contract, as applicable, and on an annual basis thereafter. The Alliance offers continuing specialized education focused on the operations of Alliance's departments and programs.

IV. Effective Lines of Communication and Reporting: The Alliance has formal and routine mechanisms of communication available to Employees, Providers, and Members. The Alliance promotes communication through virtual and in person meetings, newsletters, mailings, and other verbal and written communications. The Alliance has also engaged a third party to provide a Compliance Hotline where issues can be reported. Calls are not recorded or traced, and reporters can maintain anonymity if they desire.

V. Enforcement and Disciplinary Standards: The Compliance Program encourages a consistent approach related to the reporting of compliance issues and adherence to Policies and Procedures. It requires that disciplinary mechanisms are consistently enforced throughout the organization.

VI. Effective System for Routine Monitoring, Auditing, and Identification of Compliance Risks: The Alliance has a continuous monitoring and auditing process related to its operations and its subcontractors. Risk areas are identified through an operational risk assessment as well as by examining information collected from monitoring and auditing activities.

VII. Procedures and Systems for Response and Remediation: Once an offense has been detected, the Alliance is committed to taking all necessary steps to respond appropriately to the offense and to prevent similar offenses from occurring. The Alliance makes referrals to external agencies or law enforcement as appropriate for further investigation and follow-up.

CODE OF CONDUCT

The Code of Conduct details the fundamental principles, values, and ethical framework for business practices within and applicable to the Alliance. The objective of the Code of Conduct is to articulate compliance expectations and broad principles that guide Employees in conducting their business activities in a professional, ethical, and legal manner. The Code of Conduct is approved by the Alliance Board and is distributed to Employees, and Subcontractors upon appointment, hire, or the commencement of the contract. The Code of Conduct is reviewed and updated when a material change occurs or no later than once every three (3) years. New Employees are required to sign an attestation acknowledging receipt, review, and their agreement to abide by the standards set forth in the Code of Conduct within ninety (90) calendar days of the appointment, hire, or commencement of the contract, and annually thereafter.

All Subcontractors are required to implement a Code of Conduct or utilize the Alliance's Code of Conduct and disseminate it to their staff within 90 days of contracting with the Alliance and annually thereafter. All managers are required to discuss the content of the Code of Conduct with Contractors under their immediate supervision during contract negotiations for the purpose of confirming the Contractors' understanding of the Alliance's Code of Conduct. Contractors are encouraged to disseminate copies of the Alliance's Code of Conduct to their employees, agents, and subcontractors that furnish items or services to the Alliance and/or its members.

Compliance with Policies and Procedures

Policies and Procedures are written to help provide structure and guidance to the operations of the organization and to ensure that the Alliance stays current with contractual, legal, and regulatory requirements. Employees are responsible for complying with all Policies and Procedures. At least annually, the Alliance staff reviews the Policies and Procedures, and updates them as needed. The Alliance's Administrative Oversight Committee (AOC) reviews and approves proposed changes and additions to the Alliance's Compliance Policies and Procedures and others as determined by the Leadership Team. Operational/Department Policies and Procedures are approved by the Alliance Managers and Directors. These Policies and Procedures are available to all Employees through the Alliance's intranet.

Compliance Policies and Procedures include but are not limited to the following:

- Commitment to comply with all federal and state standards.
- Compliance expectations
- Guidance to Employees and others on dealing with potential compliance issues.
- Guidance on how to communicate compliance issues to appropriate staff.
- Description of how potential compliance issues are investigated and resolved.
- A commitment to non-intimidation and non-retaliation due to good faith participation in the Compliance Program.

OVERSIGHT

Governing Body

In its capacity as Governing Body, the Alliance Board decides on major policies and oversees the administration of the organization. The Board is made up of major stakeholders, including Alliance Members, local physicians, hospital and clinic representatives, and labor representatives. Board Members are appointed by the Alameda County Board of Supervisors. The Board exercises oversight over the implementation and effectiveness of the Compliance Program by:

- Delegating compliance oversight responsibilities to the Compliance Advisory Committee, to include providing at least two Board members to serve as committee members.
- Requiring regular reports from the Compliance Advisory Committee to the Board on its activities
- Approving the Code of Conduct and the Compliance Plan
- Understanding the Compliance Program Structure through training and education
- Remaining informed about compliance enforcement activity from external agencies, notice letters and other formal actions as needed.

Compliance Advisory Committee

The Compliance Advisory Committee is a Standing Committee of the Board, subject to open meeting laws, with a voting membership composed of Board Members as well as the CCO. The Compliance Advisory Committee meets monthly to discuss compliance-related topics. The Compliance Advisory Committee subsequently provides updates and makes recommendations to the Board of Governors and the CEO on the Alliance's Compliance Program and related subject matter. The Compliance Advisory Committee is responsible for the following functions:

- Reviewing development of the Compliance Program and Code of Conduct and recommending their approval to the Board
- Reviewing and recommending actions regarding the Alliance's regulatory compliance audit results and outcomes
- Reviewing and recommending action regarding subcontractors, their regulatory compliance, audit results and outcomes
- Reviewing compliance updates and providing reports on oversight activities to the Board as necessary

Chief Executive Officer

The Chief Executive Officer is responsible for the ongoing operation of Alliance services and products to ensure financial integrity and viability and that its goals and objectives are achieved. The CEO is accountable to the Alliance and Board of Governors for the implementation of Corporate and Board policies and directives and recommends any changes needed in administration, operation, or policy.

Chief Compliance Officer

The CCO coordinates and communicates all assigned compliance activities and programs and implements and monitors the day-to-day activities of the Compliance Program. The CCO reports directly to the CEO and the Compliance Advisory Committee on the activities and status of the Compliance Program. Furthermore, the CCO ensures that the Alliance meets all state and federal regulatory and contractual requirements.

The CCO interacts with the Alliance Board, CEO, Executive Staff, departmental management, Alliance Subcontractors, legal counsel, state and federal representatives, and others as required. In addition, the CCO supervises the Alliance Compliance Department, which includes professionals with expertise and responsibilities for the following areas: Regulatory Affairs, Delegation Oversight, Audits and Investigations, Privacy, and Legal Services. The CCO's full job description is available upon request.

The Chief Compliance Officer shall ensure that:

- The Code of Conduct and Compliance Policies and Procedures are developed, implemented, and distributed to all employees.
- The Compliance Program is reviewed and updated if needed at least annually based on changes in the Alliance's needs, regulatory requirements, and applicable law.
- The Alliance's employee attestations confirming receipt, review, and understanding of the Code of Conduct are obtained at the time of hire.
- An appropriate education and training program that focuses on elements of the Compliance Program, including but not limited to information on Medi-Cal, Health Insurance Portability and Accountability Act (HIPAA) and Fraud, Waste, and Abuse (FWA), is implemented and provided to Employees.
- Subcontractors implement education and training for their staff involved in Medi-Cal, including information about the Alliance's Compliance Program
- All data submitted to regulatory agencies is accurate and in compliance with reporting requirements.
- An annual work plan is developed in cooperation with the Compliance Committee that provides for the on-going development and implementation of the Compliance Program
- Effective lines of communication are instituted; communication mechanisms such as telephone hotline calls are monitored; and complaints are investigated and treated confidentially.
- Inquiries and investigations with respect to any reported or suspected violation or questionable conduct including the coordination of internal investigations and investigations of Subcontractors are:
    - Initiated and completed in a timely manner.
    - Reported to the appropriate organization, such as Department of Managed Health Care (DMHC), Department of Health Care Services (DHCS), other organizations, and/or law enforcement, as necessary.
    - Appropriate disciplinary actions and Corrective Action Plans (CAPs) are implemented.
- Documentation is tracked and maintained for each report of potential non-compliance, discrimination, or FWA, from any source, including CAPs or disciplinary actions

taken.

Compliance Committee

The Compliance Committee is a functional committee responsible for overseeing and monitoring the performance of the Compliance Program by providing an avenue of communications and oversight throughout the organization. The CCO or their designee serves as Chair, additional members include the CEO, Executive Staff, and Directors. This ensures the Committee's ability to act and foster a culture of compliance throughout the organization. The Compliance Committee meets at least quarterly, and is responsible for the following:

- Fostering a culture of compliance that reinforces the principles of the Alliance Code of Conduct
- Providing support for the Compliance Program, including strategies to promote compliance and detection of potential non-compliance violations
- Reviewing and approving Policies and Procedures in order to meet regulatory requirements.
- Prioritizing the compliance activities based on auditing and risk assessments performed as part of the Compliance Program
- Reviewing the risk areas and the steps taken to mitigate the identified risks

The Subcontractor & Delegation Oversight Committee (SDOC) is a subcommittee of the Compliance Committee that oversees Subcontractor agreements and responsibilities. The Subcontractor & Delegation Oversight Committee works to ensure compliance with Subcontractor requirements set forth by state and federal regulations, contractual and accreditation requirements, as well as internal standards.

The CCO or their designee serves as Chair. Subject Matter Experts (SME) from internal departments report on Subcontractor performance and activities related to their operational areas. Issues that arise are escalated as appropriate. The Subcontractor & Delegation Oversight Committee provides a summary of its activity at every meeting of the Compliance Committee. Regulatory findings are forwarded to the Compliance Advisory Committee. The Subcontractor & Delegation Oversight Committee shall meet at least quarterly.

Executive Staff

The Executive Staff shall:

- Ensure that the CCO is integrated into the organization and is given the credibility, authority, and resources necessary to operate a robust and effective Compliance Program
- Receive regular reports from the CCO on risk areas facing the organization, the strategies being implemented to address them and the results of those strategies.
- Be advised of all state and federal compliance and enforcement findings and activity, including audit findings, notices of non-compliance, and formal enforcement actions.
- Participate in corrective actions and responses as appropriate

TRAINING

The Alliance provides general and specialized compliance training and education, as applicable to Employees and in alignment with 42 CFR §422.503(b)(4)(vi)(C), Medicare Managed Care Manual Chapter 21. Required courses include the Code of Conduct, compliance obligations, relevant laws, HIPAA, FWA, and Cultural Sensitivity and Competency. The Alliance uses web-based training courses that emphasize commitment to the Compliance Program. Trainings are updated to ensure that Employees are kept fully informed about changes in procedures, regulations, and requirements. The CCO, or their Designee is responsible for coordinating compliance education and training programs and ensuring that records showing the completion of training requirements are documented and maintained.

Employees are expected to complete compliance training within 90 calendar days of hire and annually thereafter. New Board members are expected to complete compliance training within 90 days of appointment and annually thereafter.

New employees and newly appointed board members receive a copy of the Compliance Plan and Code of Conduct during compliance training and must attest that they have read and understood it. Compliance trainings for Board of Governors, employees, staff, trainees, vendors, and contractors include information regarding:

- HIPAA
- FWA
- Cultural Competency and Sensitivity
- Discrimination
- Anti-Harassment
- Code of Conduct
- Compliance Plan

Employees may receive additional compliance training as is reasonable and necessary based on material changes in laws and regulations, and/or job responsibilities.

Federal guidance specifically requires that all Subcontractors receive general compliance training, and in light of this requirement, Subcontractors are informed of their obligation to provide compliance training to their employees. A review of training documents and confirmations is conducted as part of the annual Subcontractor audit.

Documentation

Documentation requirements related to the training and education program are addressed in the following manner:

- Annual training materials for HIPAA and FWA are assigned through a web-based tool. The Compliance Department tracks completion of those trainings.
- Cultural Competency and Sensitivity training is provided annually through a webinar, created by the Diversity, Equity, and Inclusion Committee. Completion is tracked and recorded by the Health Education and the Compliance Departments

- Supplemental or Ad-Hoc training participation is tracked and monitored by the Compliance Department

All Compliance Program training documents are retained in accordance with the Alliance's Document Retention Policy. (CMP-012 - Documentation, Retention and Destruction Policy)

EFFECTIVE LINES OF COMMUNICATION

The Alliance is committed to maintaining effective and open lines of communication to ensure that all employees, contractors, and first-tier, downstream, and related entities (FDRs) are kept informed of regulatory updates and CMS communications, including but not limited to Health Plan Management System (HPMS) memos, policy changes, and other guidance issued by CMS.

Effective lines of communication are established to ensure confidentiality between the CCO, members of the Compliance Committee, the Board members, employees, subcontractors, and downstream entities. All employees are encouraged to discuss compliance issues directly with their department managers or the Compliance Department. It is made clear, via the Code of Conduct and regular training, that Employees are required to report compliance concerns and suspected misconduct or violations of law.

The CCO posts information such as Policies and Procedures, the Code of Conduct, and the Compliance Plan, on the Alliance's intranet. Access to the intranet is available to all employees. Additional information is posted as needed to update staff on changes in laws or regulations. The CCO also informs the Board of any relevant federal and state fraud alerts, policy letters, new and pending legislation reports, updates, and advisory bulletins, as necessary.

Establishment, Publication of Employees Reporting Obligations, and an Overview of the Reporting Hotline

All Employees have an obligation under the Compliance Plan to report all suspected violations, unethical behavior, questionable conduct, or practices. Reports can be made verbally, or in writing, to any department managers or the Compliance Department. In the event any person wishes to remain anonymous, they may use the Alliance's Confidential Hotline, described below, to report compliance concerns. The purpose of the hotline is to ensure that there is an effective line of communication for compliance issues between the Alliance, Employees, and any other interested parties.

Compliance Hotline

The Alliance has established a Confidential Compliance Telephone Hotline (Compliance Hotline) for the Alliance Employees and any other interested parties to report any suspected violations of law, the Compliance Plan, and/or questionable or unethical conduct or practices including, but not limited to the following:

- Incidents of FWA
- Criminal activity (kickbacks, embezzlement, theft, etc.)
- Conflict of interest issues
- Code of Conduct violations
- Misconduct or Inappropriate Behavior
- Discrimination
- HIPAA and/or PHI violations

- Harassment
- Retaliation

The Alliance uses a national hotline organization to administer its Compliance Hotline. The Compliance Hotline is a live twenty-four-hour-a-day telephone line and reporting website 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. A caller to the Compliance Hotline is initially greeted by a pre-recorded message that provides information regarding Compliance Hotline procedures and the caller's right to anonymity. Calls to the Compliance Hotline are not recorded or traced.

The national hotline organization operator asks the caller several questions relating to the reported incident, such as the time, date, and location where the issue took place, as well as any other pertinent information. All reports are referred to The Alliance's Designated Individual and investigated. Follow-up calls may be scheduled; however, information regarding the investigation and status of any action taken relating to the report may not be available to the caller.

The Compliance Hotline phone number is 1.844.587.0810. The Alliance publicizes the Compliance Hotline to Employees via e-mail notice and posting in prominent common areas. It is also posted on The Alliance's intranet, and prominently on the Alliance's website.

Member Rights Regarding Grievances and The Alliance Nondiscrimination Practices

A Member or potential member is not obligated to file a Grievance with a Provider, or with the Alliance, before filing with the DHCS Office of Civil Rights or the U.S. Department of Health and Human Services Office for Civil Rights. The Alliance's website informs members that grievances may be filed directly with the DHCS Office of Civil Rights and the U.S. Department of Health and Human Services Office for Civil Rights. The Alliance provides their contact information. The Alliance instructs subcontractor's that their website must inform members that grievances may be filed directly with the DHCS Office of Civil Rights and the U.S. Department of Health and Human Services Office for Civil Rights. The Alliance instructs subcontractors that they should provide the correct contact information.

Members are also informed of their right to ask for an Independent Medical Review (IMR) which allows an outside reviewer that is not related to The Alliance to review their case, and that they can also ask for a State Hearing where a judge will review their case. Members are informed of the contact information that is needed for them to pursue either an IMR or a State Hearing. They are informed that they can ask for both an IMR and State Hearing at the same time. Members are also informed that they can also ask for one before the other to see if it will resolve their problem first. They are informed that if they ask for a State Hearing first, and the State Hearing has already taken place, then they cannot ask for an IMR as the State Hearing has the final say. They are informed that they will not have to pay for an IMR or State Hearing. Members are also provided with contact details for Bay Area Legal Aid and the Legal Aid Society.

Members are informed that Discrimination is against the law. The Alliance follows federal and state civil rights laws, and does not discriminate, exclude people, or treat them differently because of race, color, national origin, age, disability, or sex.

In accordance with federal and state laws and regulations, member discrimination grievances are addressed by a designated Discrimination Grievance Investigator in a fair, respectful, timely, consistent, and culturally/linguistically appropriate fashion. These grievances should be resolved within

the same time as regular grievances, and a copy of the relevant information is sent to the State within 10 days of the completion of the investigation.

As well as being displayed on the website of The Alliance and its subcontractors, information detailing member rights, and The Alliance's nondiscrimination policy, along with information regarding what services The Alliance offers to assist members with disabilities, is mailed to the member within five days of receipt of a formal complaint and at the resolution of the complaint, which should be no more than thirty days from the date of receipt. Both letters also contain the IMR, State Hearing and the other information described above.

FRAUD, WASTE AND ABUSE

The Alliance maintains a robust FWA plan that defines the Alliance's approach to detecting, preventing, and deterring FWA.

In accordance with Medicare Part C & D FWA Guidance and 42 CFR §422.503(b)(4)(vi)(D), the Alliance has partnered with a nationally recognized leader in the field of software solutions for FWA detection and prevention to complement our ongoing efforts to combat these issues. This software solution platform provides The Alliance with analytics and data that allows FWA investigators to quickly respond to threats, monitor the claims procedure, and provide other actionable intelligence. It also provides the ability to quickly integrate new and emerging fraud rules and trends.

A summary of FWA cases is provided to the Compliance Committee, these cases are reviewed to determine potential actions by The Alliance. These can include whether there is a need for external assistance, or to provide a determination that FWA has not occurred.

All reports made either in writing, or verbally, of suspected compliance violations, unethical or illegal conduct, including those referred by regulatory and/or investigating government agencies, are investigated. These reports are subject to review and investigation by the CCO, or Designees and/or the Compliance Committee, in consultation with legal counsel.

DISCIPLINARY STANDARDS

Conduct Subject to Discipline

Alliance Employees may be subject to discipline up to and including termination for failing to participate in The Alliance's Compliance efforts. All new and renewing contracts include a provision that clarifies that a contract can be terminated because of a violation. The following are examples of conduct subject to enforcement and discipline:

- Failure to perform any required obligation relating to the Compliance Program or applicable law, including conduct that results in violation of any federal or state law relating to participation in federal or state health care programs.
- Failure to report suspected violations of the Compliance Program or applicable law to an appropriate person or through the Compliance Hotline.
- Conduct that leads to the filing of a false or improper claim or that is otherwise responsible for the filing of a claim in violation of federal or state law.

Disciplinary Standards for Medicare Part C and D Non-Compliance

Alliance Employees may be subject to discipline for failure to comply with CMS rules under a zero-tolerance

policy, in alignment with Chapter 9 of the Prescription Drug Benefit Manual and Chapter 21 of the Medicare Managed Care Manual. Enforcement of such standards and disciplinary actions consistently applies equally to all parties involved, including but not limited to employees, contractors, and first tier, downstream or related entities (FDR)s. Violations will be reported to CMS or other regulatory authorities, as necessary.

For reference to CMS, please see 42 CFR §422.503(b)(4)(vi) and 42 CFR §423.504(b)(4)(vi)).

Enforcement and Discipline

The Alliance maintains a zero-tolerance policy towards any illegal or unethical conduct that impacts the operation, mission, or image of the Alliance. Any Alliance Employee engaging in a violation of laws or regulations may have their employment or contract terminated, depending on the nature and magnitude of the violation. The Alliance shall accord no weight to a claim that any improper conduct was undertaken "for the benefit of The Alliance." Illegal or unethical conduct is never for The Alliance's benefit and is expressly prohibited.

The standards established in the Compliance Program must be fairly and consistently enforced. One method by which this is achieved is through disciplinary proceedings. These shall include but are not limited to the following:

- Prompt initiation of education to correct the identified problem.
- Disciplinary action, if any, as may be appropriate given the facts and circumstances of the investigation including oral or written reprimand, demotions, reductions in pay, and termination.

In determining the appropriate discipline or corrective action for any violation of the Compliance Program or applicable law, the Alliance does not take into consideration a particular person's or entity's benefit, economic or otherwise, to the organization. All Employees are aware that violations of applicable laws, regulations, or unethical behavior, could potentially subject them and/or The Alliance to civil, criminal, or administrative sanctions and penalties. Further, violations could lead to The Alliance's suspension or exclusion from participation in federal and/or state health care programs. All actions taken with regards to enforcement or discipline will be documented.

Self-Reporting

Alliance Board of Governors, employees, staff, trainees, vendors, and contractors are encouraged to report their own potential wrongdoing; however, they may not use any such report to insulate themselves from the consequences of their own violations or misconduct. Discipline shall not be increased because an Employee has reported their own violation or misconduct. Prompt and complete disclosure may be considered as a mitigating factor in determining disciplinary measures.

The Alliance makes appropriate referrals or reports to The Department of Health Care Services (DHCS) Medi-Cal Audits and Investigations Division; Department of Division; The Department of Managed Health Care (DMHC), The Office of Inspector General (OIG); The Centers for Medicare and Medicaid Services (CMS); The California Department of Public Health (CDPH); The Medical Board of California; The National Practitioner Data Bank (NPDB); the Healthcare Integrity and Protection Data Bank and other agencies, as appropriate; or law enforcement for further investigation and follow-up of cases.

Self-Reporting to CMS

In accordance with 42 CFR §422.504(m) and 42 CFR 423.504(b) for Medicare Parts C and D compliance, the Alliance is committed to self-reporting non-compliance to CMS through effective procedures to develop, compile, evaluate, and report information to CMS in the time and manner that CMS requires. The Alliance complies with the reporting requirements and technical specifications described, and the required level of reporting, timeframes, deadlines, and specific data elements for each reporting section as required.

The Regulatory Affairs Team is responsible for reporting non-compliance to CMS, as outlined in the processes found in the Critical Incident Reporting Policy and Procedure.

Confidentiality, Non-Intimidation and Non-Retaliation

The Alliance takes all reports of suspected violations, unethical or questionable conduct, or discriminatory practices seriously. Verbal communications via the Compliance Hotline and written or verbal reports to department managers or anyone designated to receive such reports shall be treated as privileged and confidential to the extent permitted by law and circumstances.

The Alliance's Open-Door Policy encourages Employees to discuss issues directly with department managers, the CCO, other Leadership Team members, members of the Compliance Committee, or the CEO. These channels of communication provide for confidentiality to the extent allowed by law.

The Alliance maintains and supports a Non-Intimidation and Non-Retaliation policy which prohibits any retaliatory action against Employees or any other party for making a formal report in good faith. This includes Qui Tam relators who make a report under federal law or under The California False Claims Act. The Plan shall not prevent, discourage or discipline a network provider or employee for informing an enrollee or subscriber about the timely access standards.

Further, the compliance team is mandated by the Compliance Plan to be allowed to act independently of operational and program areas, without fear of repercussions for uncovering deficiencies or any other violation thus allowing free and fair investigations.

Alliance Employees shall not prevent or attempt to prevent any interested party, from communicating or reporting, via the Compliance Hotline or any other mechanism. If an employee attempts such an action, they will be subject to disciplinary proceedings.

The non-tolerance for retaliation and harassment is described in the Alliances Policies and Procedures and reviewed by Alliance Employees in the annual compliance training. The Alliance takes violations of the policy on non-intimidation and non-retaliation seriously; the CCO reviews disciplinary and other corrective actions for such violations with the Compliance Committee, as appropriate.

Credentialing and Recredentialing

The Alliance requires that every network Provider is credentialed according to appropriate standards before delivering care to Alliance members and is re-credentialed at least every three years.

The Alliance reviews Providers against appropriate exclusion lists to ensure that they are not excluded, suspended or otherwise ineligible to participate in federal and/or state healthcare programs.

The Alliance requires that potential Providers disclose their Credentials and any potential conflicts of interest as part of the employment, contracting, or appointment process. When Providers receive notice of any suspension, exclusion, debarment, or felony conviction during the period of employment,

contract, or appointment they are required to immediately disclose this to the Alliance.

The Alliance also mandates that Providers complete credentialing to comply with the Alliance's requirements with respect to their relationships with subcontracted Providers. This review is conducted prior to employment or contractual engagement of a person or entity and regularly thereafter, according to Policies and Procedures.

The Credentialing Department verifies the Providers status within thirty (30) calendar days of release of information. Verification sources are queried in the third week of every month for the prior 30-day period and include:

- HHS Officer of Inspector General Cumulative List of Excluded Individuals. and entities (LEIE)
- GSA System for Award Management (SAM.gov)
- CMS Preclusion List
- Medicaid Sanctions and Reinstatement Report
- Medi-Cal Provider Suspended and Ineligible list (EPLS)
- Providers may not be listed on the Restricted Provider Data (RPD)
- Providers may not be listed on the Social Security Administration's Death Master File

All licensed Providers who provide care to Alliance members must meet the Alliance's credentialing criteria and standards to be accepted and must maintain good standing in the Alliance network. The Alliance's standards are based on federal and state requirements and comply with the DHCS, CMS, DMHC, and The National Committee for Quality Assurance (NCQA) standards and guidelines. The credentialing process ensures that Providers are properly licensed and certified as required by state and federal law.

The Alliance monitors, on an ongoing basis, Providers Medicare and Medicaid sanctions, licensure sanctions or limitations, and participation status in federal and state programs for contracted Providers between recredentialing cycles. The Alliance also monitors member complaints and identifies adverse events and makes interventions for poor quality care on an ongoing basis.

If a practitioner has been (a) convicted of a crime involving fraud or abuse of the Medi-Cal program, or (b) is suspended from the Federal Medicare program for any reason, they are notified in writing by the Alliance Credentialing Department of automatic suspension from all Alliance participation and that they are not entitled to a hearing under the California Administrative Procedures Act.

Background Checks

The Alliance has implemented Policies and Procedures relating to internal and external background checks for specified potential or existing Employees as may be required by law and/or deemed by The Alliance to be otherwise prudent and appropriate.

If it is determined that the individual should be screened out because of the background results, the following actions will be completed:

- Notify the individual that they have been screened out because of background check results.
- Provide the individual with an opportunity to demonstrate that they should not be excluded due to particular circumstances.
- Determine if the additional information provided warrants and exception to the exclusion and shows that the exclusion is not job related and consistent with business necessity.

- If it is determined that the applicant should be excluded from the job based on the above, Human Resources (HR) will:
- Document the Adverse Employment Decision and request an adverse action form (provided by an independent third party).
- Notify HR who will confirm or reverse the recommendation.
- Send the appropriate communication to the applicant.
- Notify the hiring manager of the determination; however, details of the results will not be communicated or discussed.

If the applicant is not excluded, HR will make the hiring recommendation to the hiring manager based on the information gleaned.

All background checks are reviewed and signed off by the Chief Human Resource Officer. Particular circumstances of incident/offense are reviewed by the Chief Human Resource Officer, and they may request judgment of Legal Counsel. Signed off background check with justification will be filed in the employee's Personnel File and will be retained in strict confidence by HR.

Internal Background Check

This is the process followed by HR once an individual is selected as the final applicant for a position with The Alliance. HR will notify the individual that they are the final applicant and request the required three professional references. If the applicant has been in their current position at least one year, the Alliance will allow the applicant to submit one recent performance evaluation on file as one of the three required references.

HR will check references, including verification of professional licenses, driver's license, and insurance when applicable. If there is reason to doubt the validity of the reference, or if the reference revealed job-related issues which bring into question the suitability of the candidate, in addition to, if a reference is non-responsive or unavailable, HR will request additional references. Should HR receive any unfavorable or questionable information during the references, the Hiring Manager, Area Chief and Director will be notified of such information.

External Background Check

This is the process followed by HR once an individual is selected as the final applicant for a position with the Alliance and has satisfied the requirements of the Internal Background Check.

The candidate is made aware in the offer letter that employment is contingent on passing the background check and successful completion of reference checks. HR will send the candidate the necessary authorization and notice documents. For any previous Alliance employees who apply for rehire within 90 days of separation of employment the background check will be waived.

The required background check includes the areas listed below. Background checks will be conducted in all counties and/or states in which the employee has resided, and for all aliases, unless otherwise indicated.

The requirements listed below apply to all jobs:

- Civil-county level screening– tax liens/bankruptcies/fines, and any items that are on record.
- Criminal: federal, and all states and counties where the individual has resided

- Education: Only the highest education requirement will be verified.
- Licensure: All jobs that require a professional license or certification
- OIG (national sanctions): All jobs
- Employment: Only the most recent employment will be verified

For jobs that require the employee to have a driver's license as identified in the job description there will be verification of good standing through the Department of Motor Vehicles (DMV). The Alliance will conduct Pre-Employment Exams, if applicable to the job requirements, including drug and alcohol testing if deemed necessary.

Should the third-party vendor not be able to verify employment or education, the Alliance will request W-2s, transcripts or letters from the State Department of Education which will be used in a further attempt to verify the accuracy of the information provided.

MONITORING AND AUDITING

The CCO and/or the Compliance Committee will utilize the annual Risk Assessment to direct the Alliance's Compliance and operational staff in performing monitoring and auditing functions for the organization to ensure compliance with applicable laws and the Compliance Plan. They report, investigate and when necessary and appropriate, correct any inconsistencies, suspected violations, or questionable conduct within the organization.

In addition, the CCO develops monitoring and auditing Policies and Procedures that are reviewed by the Administrative Oversight Committee (AOC) annually.

Monitoring and Auditing: Medicare Operations

To comply with CMS regulations outlined in 42 CFR §422.101(f), the Alliance will conduct regular audits of D-SNP care coordination processes, focusing on the integration of Medicare and Medicaid services. These audits will include the review and management of individualized care plans and initial health risk assessments using a comprehensive risk assessment tool that CMS may review during oversight activities, the effectiveness of care coordination activities, and compliance with CMS' Model of Care requirements for dual-eligible members.

The CCO and/or the Compliance Committee will utilize the annual Risk Assessment to direct the Alliance's Compliance and operational staff in performing monitoring and auditing functions for the organization to ensure compliance with high-risk Medicare operations, such as but not limited to claims, grievances, and appeals. The Risk Assessment is used to identify high-risk areas and the auditing of Medicare Part C and D operations using CMS Audit Protocols, for the purpose of developing an annual Audit and Monitoring Plan using the Risk Assessment.

Monitoring

Monitoring is on-going and meant to ensure internal processes are working as intended. Monitoring is performed regularly or on an ad hoc basis. For example, Providers are monitored by the Alliance to verify that their information is accurate and up to date.

The Alliance monitors, on an ongoing basis:
- Provider Medicaid sanctions
- Licensure sanctions and limitations
- Participation status in federal and state programs for providers during recredentialing cycles

The Alliance investigates any complaint it receives, written or verbal, in accordance with local, state, and federal laws and guidelines. The Alliance identifies adverse events and takes appropriate measures to resolve issues, including referral to law enforcement or other agencies when necessary.

Auditing is completed by compliance staff, acting independently of operational areas, and is a more formal and objective approach to evaluate and improve the effectiveness of the Alliance processes and to ensure oversight of Employee and Subcontractor activities.

Risk assessment tools are used to conduct a baseline assessment of The Alliance's major compliance and FWA risk areas. This includes the Medi-Cal and Group Care lines of business, such as quality improvement, appeals and grievances, credentialing, utilization management, claims, and cultural and linguistic services. The risk assessment is completed annually and updated on a quarterly basis as needed.

Oversight of Subcontractor Activities

The Alliance delegates certain functions and/or processes to its Subcontractors. These include:

- **Utilization Management** for Medi-Cal and Group Care
- **Credentialing** for Medi-Cal and Group Care
- **Claims** Medi-Cal and Group Care
- **Call Center** for Medi-Cal and Group Care.
- **Case Management** for Medi-Cal and Group Care
- **Cultural and Linguistic Services** for Medi-Cal and Group Care.
- **Provider Training** for both Medi-Cal and Group Care.

Subcontractors and those entities downstream of them are required to meet all contractual, legal, and regulatory requirements and comply with the Alliance's Policies and Procedures and other guidelines applicable to delegation reporting and the Compliance Plan. The Alliance regularly reviews all Policies and Procedures relevant to subcontracted functions. The Alliance maintains oversight of these functions through the Subcontractor and Delegation Oversight Committee and conducts annual and or focused ad hoc audits of Subcontractors and other entities as applicable. The results of the reviews and notices/disclosures are provided in periodic reports to the CCO.

Auditing

The CCO develops an auditing work plan, which is approved by the Compliance Committee, to address risks, including, but not being limited to, areas of risk identified in the OIG's Annual Work Plan, by Medi-Cal, and from other sources. Focused audits are also conducted based on reports from The Alliance's regulators including DHCS and DMHC.

Internal Auditing

An annual auditing plan is developed by the Compliance Department and includes:

- Internal audit schedule
- Audit report, including:
    - Audit objectives
    - Scope and methodology
    - Findings

    - Recommendations
- Audit staffing
- Approval, monitoring, and validation of CAPs

The creation of the annual audit plan is based on risk assessment, as well as input from internal departments, to determine which areas will have the most effect on the operation of the Alliance. The Compliance Committee has input into the priority of the monitoring and audit strategy. In determining risk areas, the Alliance reviews, at a minimum, but not limited to:

- DHCS and DMHC guidance
- NCQA standards and survey results
- Audit findings from external reviewers, including DMHC, DHCS and CMS
- Enforcement notices from state or federal regulatory agencies
- Auditing and monitoring findings from internal reviews, including department and Compliance, internal audits, internal operational dashboards, metrics, and scorecards.
- Internal workplans
- Member interactions with Alliance departments, including Grievance and Appeals, Member Services, and Claims
- Self-identified issues reported by internal departments.
- New regulatory requirements
- New operational systems or practices
- CAPs from previous audits
- Compliance Department recommendations

All compliance actions taken are monitored and tracked to evaluate the success of implementation efforts. Audits may also include follow-up reviews of areas previously found non-compliant to determine if the corrective actions taken have fully addressed the underlying problem.

Audit Review

The CCO submits regular reports of all auditing and corrective action activities to the Compliance Committee. When necessary, the Alliance informs the appropriate agency including but not limited to federal or state authorities of aberrant findings.

Prompt Response to Compliance Issues

The Alliance is committed to responding to compliance issues thoroughly and promptly and has developed Policies and Procedures to address the reporting of, and responding to, these issues. If an Employee becomes aware of a suspected violation or questionable or unethical conduct the Employee must notify an appropriate Alliance staff member immediately. A Board member, Subcontractor, Vendor, Consultant, or downstream entity should notify The Alliance of a suspected violation or questionable unethical conduct by reporting the concern to the CCO or CEO. Any such reports of suspected violations may also be made to the Compliance Hotline.

Compliance issues involving the CEO are referred directly to the Board. Any issue that involves a Board member is referred to the CEO.

Compliance issues involving state regulatory agencies are investigated, tracked, and reported as needed.

Annual Risk Assessment

The CCO, or Designee, will ensure that an annual comprehensive risk assessment is completed to determine the Plan's vulnerabilities and high-risk areas. Any previously identified issues, which include any corrective actions, service level performance, reported detected offenses, and/or complaints and appeals from the previous year will be factors that are included in the risk assessment. The risk assessment process, along with any reports, will be managed by the CCC, or Designee, and presented to the to the Compliance Committee for review and approval.

DOCUMENTATION

The Alliance maintains Records and Documents in accordance with all applicable statutory, regulatory, contractual, internal policies, and other requirements. The CCO has established and maintains a secure electronic filing system for the management, organization, and preservation of all compliance-related Records and Documents.

Document Retention

In accordance with the Alliance Document Retention Policy and 42 CFR §422.504(d) and 42 CFR §423.505(d), all Records and Documents are retained for a minimum of ten (10) years from the later of:

- The end of the Alliance's final contract period.
- The completion of the most recent state or federal audit or investigation conducted by CMS or any other regulatory agency. Exceptions to this rule are documents subject to a legal hold, which may be retained longer, or documents determined to be permanent, which will be retained indefinitely, and in case of ongoing investigations and audits.

Documents will be destroyed securely after the required retention period.

APPENDICES

Appendix A—Code of Conduct
Appendix B—Privacy Program
Appendix C—Compliance Committee Charter
Appendix D—Subcontractor & Delegation Oversight Committee Charter
Appendix E—Administrative Oversight Committee Charter
Appendix F—Anti-Fraud Plan

Appendix A

ALAMEDA Alliance FOR HEALTH

Health care you can count on.
Service you can trust.

Code of Conduct

Table of Contents

CEO's MESSAGE ON COMPLIANCE

Alliance Team,

For nearly 30 years, Alameda Alliance for Health ("Alliance") has upheld a tradition serving our community with integrity and accountability. Our ongoing commitment to offer members quality health care services while meeting the highest ethical standards of business conduct continues today. In the healthcare industry, change is something we can always count on. However, our commitment to serve our members and our community with the highest level of ethical behavior remains unchanged. The Alliance's code of conduct demonstrates our organization's commitment to fulfilling our mission, vision and to our members.

As you know, trust is key to the success of any organization and ethical conduct is the foundation upon which that trust is built. Ethical conduct simply means doing the *right thing*. Most of us – if not all of us – come to work every day with the best intentions, to do the right thing, and to live by our organization's values. While the Code of Conduct does not cover every situation you may encounter, it serves as a guide to help you comply with rules and regulations that govern our organization.

The Code of Conduct is the cornerstone of the Alliance's Compliance Program. It contains the standards of behavior that each one of us is expected to observe while performing our jobs. Spelling out these standards helps us all maintain a culture of integrity and excellence.

I encourage you to read and understand our Code of Conduct and follow it every day. Thank you for your commitment to serving our members with the highest levels of integrity.

Sincerely,

Matthew Woodruff

Chief Executive Officer Alameda
Alliance for Health

The **Mission** of the Alliance - Improving the health and well-being of our members by collaborating with our provider and community partners to deliver high quality and accessible services.

The **Vision** of the Alliance - All residents of Alameda County will achieve optimal health and well-being at every stage of life.

INTRODUCTION TO THE CODE OF CONDUCT

The Board of Governors of Alameda Alliance for Health (Alliance) has adopted the Code of Conduct with respect to the business conduct and practices governing the Alliance's affairs. Unless the context otherwise requires it, a reference to "employee or employees," made hereafter, means a "governor, employee, staff, trainee, vendor or contractor" of the Alliance.

This Code of Conduct governs the manner in which employees conduct business activities on behalf of the Alliance. Employees must be familiar with this Code of Conduct and adhere to it at all times.

This Code of Conduct has been developed to create a framework of compliance with laws, regulations, and ethical standards.

The following Alliance values form the basis for this Code of Conduct:

Our Values (T.R.A.C.K.)

Teamwork: We participate actively, remove barriers to effective collaboration, and interact as a winning team.

Respect: We are courteous to others, embrace diversity and strive to create a positive work environment.

Accountability: We take ownership of tasks and responsibilities and maintain a high level of work quality.

Commitment & Compassion: We collaborate with our providers and community partners to improve the wellbeing of our members, focus on quality in all we do and act as good stewards of resources.

Knowledge & Innovation: We seek to understand and find better ways to help our members, providers, and community partners.

Although it may not address all questions or concerns, the Code of Conduct is a resource meant to address the most common aspects of employee conduct. This document, along with the Alliance's Compliance Program and the Employee Handbook, promote a culture of ethical behavior, prevention, detection, and resolution of situations.

ETHICS

The Alliance is committed to the highest standards of business ethics and integrity. The Alliance will always fairly and accurately represent itself in all business relationships. The Compliance Program and related policies and procedures help ensure that the business activities of the Alliance reflect these high standards.

Equal Opportunity and Treatment

The Alliance is committed to creating a workplace that, at all times, is free from harassment and discrimination, where all employees respect each other, and abide by this Code of Conduct.

The Alliance is committed to maintaining a safe and professional working environment for all employees, ensuring; fairness, dignity, and respect regardless of race, color, creed, religion, sex, gender, national origin, disability, marital status, age, sexual orientation, and public assistance status or any other basis protected by federal, state or local law, ordinance or regulation. In addition, good faith efforts are made to reasonably accommodate the physical and mental limitations of special disabled veterans and individuals with disabilities.

CONDUCT

The Alliance's success as an organization depends largely on its reputation as an honest and ethical company. The Alliance is committed to achieving success by fair and ethical means, prohibiting any unethical, non-competitive, and illegal business practices. The Alliance will deal fairly with members, providers, and other business associates. The Alliance will not take unfair advantage of anyone through manipulation or concealment of information, abuse of confidential information, misrepresentation of facts, or any other unfair business practice.

As an employee of the Alliance your actions are a direct reflection of Alliance business. Each employee is expected to act with honesty and integrity in a manner that is consistent with this Code of Conduct whenever acting on behalf of the Alliance. Employees will be subject to disciplinary actions for violating the principles outlined in this Code of Conduct, consistent with the Alliance's Human Resources policies and procedures.

Accurate Records

Accurate business records are important for legal, financial, government, and other reporting obligations of the Alliance. Records should always be kept in an accurate, true, and complete manner consistent with relevant record retention policies and legal requirements. Records should never be changed, tampered, falsified, or withheld and only be disposed of in a proper manner, once no longer needed or required by law or contract to maintain.

All documents, emails, and other correspondence are considered Alliance records and owned by the Alliance. Employees should use discretion and professionalism when creating Alliance records. All records must remain on Alliance property or other approved locations and may not be stored in employee homes or in other unapproved locations.

LAWS AND REGULATIONS

The Alliance is committed to and expects each employee to conduct all activities in full compliance with applicable laws, regulations, and contractual obligations. While it is difficult to know the details of these laws, if there is any doubt as to whether an activity is legal or appropriate, employees should seek clarification from Department Management, Human Resources Management or the Compliance Department.

Pursuant to CMS's requirements for having a Code of Conduct, as outlined in 42 CFR §422.503(b)(4)(vi) and the Medicare Managed Care Manual, Chapter 21, the Alliance is committed to abiding by Medicare compliance obligations, including FWA prevention, reporting, and Medicare Program integrity.

Conflicts of Interest & Disclosures

Employees are expected to use good judgment, to adhere to high ethical standards, and to avoid situations that create an actual or potential conflict between their personal interests and the legitimate business interests of the Alliance. A conflict of interest exists when an employee's loyalties or actions are divided between the Alliance's interests and those of another, such as a competitor, provider, vendor, supplier, or customer. All potential conflicts of interest must be fully disclosed to Department Management, Human Resources Management, and the Compliance Department as described in the Employee Handbook.

Confidentiality

Every employee of the Alliance must ensure the protection of all confidential information received in the course of their relationship with the Alliance. The Alliance will comply with applicable federal and state laws protecting the privacy and security of members' protected health information (PHI). Member PHI must be protected in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the California Confidentiality of Medical Information Act (CMIA), other applicable federal and state privacy laws, contractual requirements and the Alliance's policies and procedures.

The Alliance will act responsibly by maintaining the confidentiality of member information and limiting its distribution only to what is minimally necessary to appropriate authorized individuals. In addition, Alliance employees will maintain the confidential and proprietary information about the operations and plans of the Alliance, consistent with applicable legal and ethical standards.

Protection of Company Assets

Since much of the Alliance's work is publicly funded, there is an even a higher responsibility to be prudent with company assets. All employees must preserve and protect company assets by promoting their efficient and effective use. Company assets may be used only for business purposes and only by authorized employees. All employees should report any situation that could lead to loss, misuse, or theft of company assets to Department Management, Human Resources Management or the Compliance Department.

Fraud, Waste and Abuse (FWA)

FWA is harmful to the Alliance, its members, and the entire healthcare system by diverting significant resources away from necessary health care services. All employees are responsible to prevent, detect, and report suspected FWA. If FWA is suspected, report to Department Management, Human Resources Management, or the Compliance Department. The Alliance is committed to comply with CMS's Medicare obligations by satisfying FWA training requirements.

Business Relationship

The Alliance must conduct all business transactions free from solicitation or receipt of bribes, kickbacks, gifts, favors, or improper incentives. Employees of the Alliance may not offer, give, solicit, or receive anything of value to induce a referral of business. If there are any questions, please refer to Department Management, Human Resources Management or the Compliance Department.

REPORTING, QUESTIONS AND CONCERNS

The Alliance encourages and expects that all employees report any suspected violations of the standards presented in this Code of Conduct, related compliance policies, and applicable laws, statutes, rules, and regulations. Reporting systems have been established by the Compliance Department to provide a means to report violations, without fear of retaliation or retribution, which meet reporting obligations under the law. The Alliance is committed to CMS's Medicare compliance standards and obligations, including whistleblower protections and mandatory reporting protocols.

Non-Retaliation

The Alliance is committed to providing employees with the opportunity and means to report, in good faith, violations to internal and external parties without fear of retaliation. Anyone who reports a potential violation or cooperates with an investigation is protected against discrimination, intimidation, or retaliation. Any employee who retaliates against a person for filing a report or participating in an investigation is subject to corrective action up to, and including, termination of employment.

All violations should be reported consistent with the procedures described below.

HOW TO REPORT

Listed below are multiple ways to reach out for questions, concerns or for reporting suspected incidents.

All reported incidents are fully investigated and corrective action plans may be implemented for continuous monitoring until incidents are fully resolved. If necessary, incidents are reported to the appropriate regulatory agency or law enforcement.

- Email the Compliance Inbox at **compliance@alamedaalliance.org**
- Email HIPAA & Privacy incidents at **privacy@alamedaalliance.org**
- Contact the Chief Compliance Officer / Chief Privacy Officer –Richard Golfin III
    - **rgolfin@alamedaalliance.org**

    - **510.747.6245**
- Chief Human Resource Officer – Anastacia Swift
    - **aswift@alamedaalliance.org**
    - **510.373.5701**
- Report to your Department Management
- Contact any Compliance team member.

If you suspect fraud by our health plan, doctors, pharmacies, or members, please report it by:

- Calling the Alliance Compliance Department Hotline: **1.844.587.0810**
    - **Anonymous Reporting is available on the Hotline.**
- Calling the Medi-Cal Fraud and Abuse Hotline: **1.800.822.6222**
- Emailing the Alliance Compliance Department: **compliance@alamedaalliance.org**
- Visiting the website: **www.alamedaalliance.ethicspoint.com**

VIOLATIONS OF THIS POLICY

Non-conformance with this Code of Conduct will be construed as misconduct that could warrant disciplinary action, up to and including termination. The disciplinary decision will lie with management and Human Resources and shall be binding upon the employee.

ACCOUNTABILITY

Employees are required to read, acknowledge, and sign this Code of Conduct. Employees understand and agree that signing the Code of Conduct certifies that the Employee has received, read, agrees with, and will abide by, the Code of Conduct and all the Alliance policies.

EMPLOYEE ATTESTATION

I have received, I have read, I understand, and I agree to comply with the Alameda Alliance for Health Code of Conduct.

_____

PRINT EMPLOYEE'S NAME

_____ _____

EMPLOYEE'S SIGNATURE DATE

_____ _____

CHIEF COMPLIANCE OFFICER DATE

Appendix B

THE PRIVACY PROGRAM

The mission of the Privacy Office (PO) is to safeguard and maintain the integrity of protected health information (PHI) and personally identifiable information (PII) housed within the Alliance network. The PO at Alameda Alliance for Health (Alliance) provides services in 4 distinct areas:

(1) Privacy coordination and support services.

(2) Data and privacy governance.

(3) Third party vendor management; and

(4) Privacy regulatory applications.

Privacy coordination and support services:
Within the framework of privacy coordination and support services, the PO acts as a resource department for all Employees of the Alliance to:

- Deliver privacy-related guidance in a digestible format to stakeholders related to applicable privacy requirements in response to research, new product concepts, specific inquiries, and other similar tasks.
- Work with stakeholders to analyze business processes, document data flows, and/or advise on potential privacy compliance gaps.
- Coordinate with the Alliance security team through the Privacy Security Joint Taskforce (PSJT) to collaboratively problem solve and proactively address potential privacy / security concerns at the Alliance.
- Design and provide training, tools, and other resources to increase awareness and understanding of privacy regulations and Employee responsibilities.
- Coordinate incident response consultation.
- Partner with internal and external stakeholders to triage security incidents and ensure thorough investigations and mitigation plans are executed, and appropriate notices are sent upon data breach determinations.
- ensure timely notification to regulators when required by law. This includes reporting significant breaches or privacy incidents to the California Department of Health Care Services (DHCS) within 24 hours of discovery, in accordance with All Plan Letters, and to the Centers for Medicare & Medicaid Services (CMS) as required under Medicare rules. These notifications are made in coordination with Compliance, Legal, and other internal stakeholders.

Data and privacy governance:
In conjunction with the Alliance's Chief Information Security Officer and PSJT, the PO maintains privacy principles, policies, and notices given to members at the time of data collection and manages the availability, usability, accessibility, and integrity of both PHI and PII. Additionally, the PO provides a process to assess the legal, contractual, and ethical implications of the collection and processing of data, PHI, and PII, especially sensitive data.

Third party vendor management and delegation oversite:
The PO engages in a review of privacy terms and conditions including redlining and editing, providing recommendations, and, in some cases, assisting with negotiating contract language with vendors. To that end, the PO also monitors information security and privacy through customization of contract addenda and appendices to strengthen the Alliance's security and privacy stance.

In addition to contract review and negotiation, the PO supports ongoing vendor oversight activities. This includes annual privacy and security attestations, periodic risk-based reviews of vendor controls, and ensuring breach notification procedures are in place and contractually enforceable. The PO may collaborate with the Delegation Oversight team and other stakeholders to monitor compliance with privacy and security requirements and document any corrective actions needed.

Privacy regulatory applications.
In conjunction with stakeholders, the PO drafts privacy statements, data sharing agreements, and data protection assessments. As part of this program, the PO monitors, interprets, and applies privacy regulations and policies, strategizing to adapt to evolving regulatory, industry, and technology changes impacting the Alliance's compliance with sectoral and jurisdictional privacy laws and regulations. In addition, the PO triages and manages complaints related to concerns about members' privacy.

APPROACH

Privacy principles are embedded into the design of systems, workflows, and organizational operations to ensure compliance is integrated from the outset. The PO tracks and reviews a variety of privacy-related metrics to evaluate program effectiveness and identify opportunities for improvement. Key indicators include the number and severity of privacy incidents, breach response time, completion rates for employee privacy training, timelines, and findings from internal audits. These metrics are reviewed regularly to inform strategic priorities, drive process improvements, and ensure alignment with regulatory expectations. The success of the Privacy Program requires an interdepartmental partnership for consistent application of requirements across policies, procedures, and processes. Several departments and the cross-departmental (PSJT) aid in the interpretation of relevant laws and regulations and subsequent development of policies and procedures and training to ensure compliance with privacy and security requirements.

Training and education:
Led by the PO, the Alliance Compliance Department provides general and specialized compliance training and education. The PO is responsible for coordination of the Compliance training and education program as well as ensuring training and education records are maintained to meet regulatory requirements.

The security and confidentiality of member information and data are a main component of the Employee training program. All new Employees, including temporary Employees, receive this training within their first ninety (90) days of hire. Select trainings are provided to all Employees annually thereafter.

- Health Insurance Portability and Accountability Act (HIPAA)
- Fraud, Waste, and Abuse†
- Cultural Sensitivity, Diversity, Equity, Inclusion, and Belonging
- Compliance Plan
- Code of Conduct
- Diversity in the Modern Workplace
- Anti- Harassment

In addition to internal training, the PO supports education efforts for members and providers regarding privacy rights and responsibilities. This includes publishing periodic “Privacy Corner” articles in member and provider newsletters, offering guidance on accessing records or submitting privacy requests, and responding to questions or concerns related to data use.
The HIPAA Guidelines for Working Remote is distributed each year to all staff and provided to new Employees upon hire. This memo is updated each year to reflect the needs of the Alliance and outlines the requirements to protect member PHI while Employees are working outside of the office, in a remote environment.

Each year the PSJT creates and presents training on current, relevant privacy and security topics to all Employees. The training is presented individually to each department, allowing time for questions and answers. In addition, the PSJT delivers privacy and security best practices and updated requirements at two (2) All Staff meetings each calendar year. Department specific training is created and presented at the request of Department Leads.

Each month data security training is provided through the KnowBe4 training module with the use of “test” emails for Phishing. The purpose of this training is to familiarize Employees with Phishing emails that can lead to Ransomware and other security incidents at the Alliance.

Twice per year the PO provides a “Privacy Corner” article to bring awareness to relevant privacy subjects, such as member rights. This article is published in the Employee, Provider, and Member Newsletters.

The PO conducts an evaluation of the Privacy Program to assess its effectiveness and identify areas for improvement. This evaluation may take the form of an internal audit, self-assessment, or privacy gap analysis, and includes a review of policies, training effectiveness, incident response procedures, and third-party oversight. Findings are documented, tracked, and addressed through policy updates or procedural enhancements. This process supports compliance with regulatory expectations from CMS, DHCS, and OCR, and ensures the Privacy Program evolves in response to changes in regulations, technologies, and operational risks.

CONFIDENTIALITY
Every Employee at the Alliance must adhere to all requirements for confidentiality of member data as implemented by the Alliance. The Alliance ensures all Employees are aware of and abide by the laws,

regulations, contractual obligations, and other expectations as outlined in the Code of Conduct and Compliance Plan. Specific Privacy policies and procedures provide requirements for protecting the privacy and security of members' PHI and PII, company information, and other sensitive data.

The Alliance is committed in its compliance with CMS regulations on protecting member health information, as outlined in 42 CFR §422.118 for Medicare Advantage and 42 CFR §423.136 for Medicare Part D. The privacy and security of member data are safeguarded following CMS and HIPAA requirements.

Sensitive Data Handling
In addition to general privacy protections, the Alliance applies heightened safeguards to sensitive health information, including mental and behavioral health, substance use disorder (SUD) treatment, HIV status, reproductive health information, and services involving minors. Handling of such information is guided by applicable federal and state laws, including the California Confidentiality of Medical Information Act (CMIA), 42 CFR Part 2, and HIPAA regulations. Systems and workflows are reviewed to ensure appropriate consent requirements, redaction procedures, and disclosure tracking are in place. Special attention is given to sensitive condition flags, member privacy requests, and data sharing with third parties or legal entities to maintain compliance with evolving state and federal guidance.

The Privacy policies are available to all Alliance staff through an online repository, Navex, and upon request to external parties including vendors, contractors, and members.

- CMP-001 Compliance Program
- CMP-004 Privacy Officer
- CMP-005 Minimum Necessary Use and Disclosures
- CMP-006A Access of Personal Health Information - Member Requests
- CMP-006B Amendment of PHI – Member Request
- CMP-007 Release of Personally Identifiable Information to Plan Sponsors
- CMP-008 Member Rights to Release Protected Health Information
- CMP-009 Accounting for Individual Disclosures
- CMP-010 Notice of Privacy Practices
- CMP-011 Business Associate Agreements
- CMP-012 Document Retention and Destruction Policy
- CMP-013 HIPAA Privacy Reporting
- CMP-015 Minor Consent to Medical Care
- CMP-016 HIPAA Privacy Rounds
- CMP-018 Employee Sanctions
- CMP-025 HIPAA Remote Access Requirements
- CMP-026 Compliance Training and Education
- CMP-032 Offshore Arrangements
- CMP-035 Confidential Communication Requests
- CMP-036 Data Sharing Agreement Types
- CMP-044 Disclosing PHI with a Valid HIPAA Authorization
- CMP-044 HIPAA Secure Email Policy

Appendix C

Compliance Committee Charter

Purpose

The Compliance Committee's primary purpose is to:

- Oversee and approve the Alliance's Compliance Program activities and monitor and evaluate the Alliance's compliance with all regulatory standards, to include, but not limited to federal, state, contractual, accreditation, and other plan requirements, as applicable;
- Support the Chief Compliance and Privacy Officer (CCO/CPO) and the Compliance Division in promoting ethical practices, regulatory progress, risk mitigation, and discussion of Compliance Program initiatives, goals, and operations;
- Provide a platform for effective communications and oversight among Plan Departments and Divisions, the Chief Executive Officer (CEO), and the Alliance Board of Governors (BOG).
- Oversee the Alliance's adherence to CMS Medicare Parts C and D compliance requirements, including assurance that the organization meets all obligations under 42 CFR §422.503(b)(4)(vi) and 42 CFR §423.504(b)(4)(vi), and that corrective actions are taken promptly to address any non-compliance identified through internal or external audits.

Responsibilities and Functions

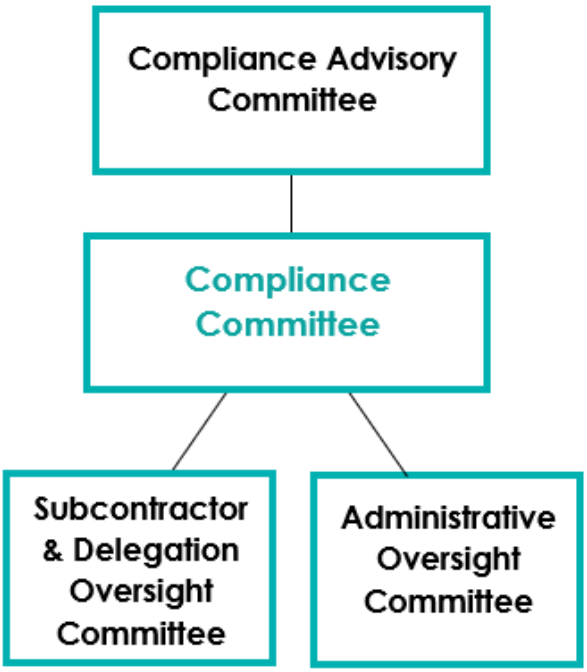
1. To foster a culture of compliance across the enterprise and model the Code of Conduct principles at the Alliance. The Code of Conduct governs the way staff, providers, the BOG, and other affiliated partners conduct business at, and on behalf of, the Alliance.
2. To ensure that the Compliance Plan, Code of Conduct and Compliance Committee charters are regularly updated and reviewed in a reasonable timespan.
3. To remain knowledgeable about issues/risks related to business at the Alliance and within the general health care industry.
4. To provide support for the Compliance Program, including implementation and discussion of strategies that promote compliance initiatives and assist in the detection of potential occurrences of non-compliance at the Alliance.
5. To prioritize and assess compliance-related activities across the enterprise, based on auditing, monitoring and risk assessment exercises performed as part of the Compliance Program and applicable rules, regulations, and policies.
6. To review risk areas and associated processes established to monitor, control, prevent and report compliance-related risks and exposures.
7. To foster and guide development of effective, compliance, cyber security, HIPAA/Privacy, and Anti-Fraud education and training programs.
8. To review Corrective Action Plans generated as a result of external regulatory review and activities, internal audits, and other risk-associated activities, including regular audits and corrective action plans related to Medicare and, to recommend further remedial steps that enhance compliance oversight and address specific concerns raised by the committee, its members, or its guests.

Committee Composition & Structure

The Compliance Committee is an operational committee of the Board Delegated Compliance Advisory Committee (CoAC). The CCO/CPO or their designee will serve as the Chair of the Compliance Committee and shall provide leadership to the Committee. The CCO/CPO may designate a qualified Director within the Compliance Division, to serve as Chair or Co-Chair, when necessary.

The voting members of the Compliance Committee may be comprised of, but not limited to, members who are at or above the director level from the following areas:

- Executive Senior Leadership Team (SLT)
- Medical Directors
- Quality
- Legal
- Operations
- Provider Services
- Grievances and Appeals
- Human Resources
- Utilization Management
- Health Equity
- Analytics
- Claims
- Integrated Planning
- Information Technology and Security
- Finance



On an ad-hoc basis and as necessary, additional staff may be designated as voting members by the Chair. A quorum is met when 50% of voting members are in attendance, to include the Chair or Co-Chair. Voting Committee members are expected to attend every session, or to designate a qualified representative from their scope of work to attend in their place, when necessary. Non-voting members will include Compliance staff.

The Subcontractor and Delegation Oversight Committee (SDOC) was established as a subcommittee of the Compliance Committee to oversee delegation agreements and responsibilities between the Alliance and its delegated entities and subcontractors. The SDOC shall meet quarterly. The Committee Chair or their designee shall present a summary of the SDOC's quarterly activities at the Compliance Committee, when possible.

The Administrative Oversight Committee (AOC) was established as a subcommittee of the Compliance Committee to oversee the Alliance's administrative affairs, functions, and processes. The Committee is responsible for facilitating the discussion of various topics and reviewing and approving policies and procedures that further the goals and objectives of the Alliance's Code of Conduct and Compliance Program. The AOC shall meet monthly, or on a schedule which the chair deems reasonable and appropriate to address the affairs of the Alliance. The Committee Chair or their designee shall present a summary of the AOC's quarterly activities at the Compliance Committee.

Meetings

The Compliance Committee shall meet quarterly. If a meeting cannot be held, the data and information from the

previous meeting shall be disclosed at the next meeting of Committee members. The Committee may meet on an ad-hoc basis, as necessary.

Reporting & Governance

Meeting minutes of the Compliance Committee must be approved by the Committee. The Compliance Committee summary of activities shall be reported to the Board of Governors, preferably to the CoAC.

Appendix D

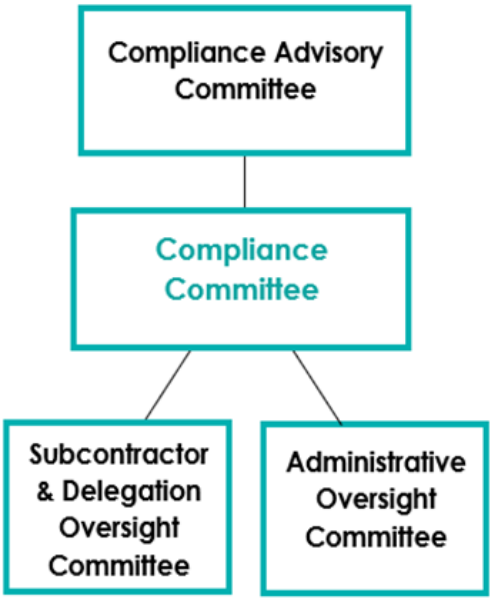
SUBCONTRACTOR & DELEGATION OVERSIGHT COMMITTEE (SDOC) CHARTER

Purpose:

The Subcontractor & Delegation Oversight Committee (SDOC) is established to oversee delegation and subcontractor agreements and responsibilities between Alameda Alliance for Health (Alliance) and its delegated entities and subcontractors. The SDOC works to ensure Alliance's compliance with delegation, subcontractor, down-stream subcontractor and vendor requirements as set forth by state and federal regulations, contractual and accreditation requirements, as well as internal Alliance standards. Issues that arise are escalated to the Chief Compliance Officer, Chief Executive Officer, and the Senior Leadership Team (SLT), as appropriate.

Composition & Structure:

The Chief Compliance and Privacy Officer (CCO/CPO) is the chair of the SDOC and shall provide leadership and oversight to the committee. The CCO/CPO may designate the Compliance Director to serve as Chair or Co-Chair of the SDOC. The SDOC is established as a subcommittee of the Compliance Committee. The SDOC will provide a summary of its activity at every meeting of the Compliance Committee.



SDOC members will include senior Subject Matter Experts (SMEs) from internal departments, who will report on delegation performance and activities related to their operational areas. The voting members of the SDOC may be comprised of, but not limited to, leadership from internal departments. On an ad-hoc basis and as necessary, the SDOC Chair may designate additional staff as voting members.

The number of voting members will be no less than fifteen (15) and no more than twenty (20). Voting committee members are expected to attend every session. If a committee member is absent, they must appoint a departmental representative to attend in their place, granting the representative voting privileges for those meetings. A quorum is met when 50% of voting members are in attendance, including the Chair or Co-Chair.

Responsibilities & Functions:

- Identify potential delegated entities and subcontractors within scope of the Department of Health Care Services (DHCS), the Department of Managed Health Care (DMHC), Knox-Keene Act, and/or the National Committee for Quality Assurance (NCQA) oversight.
- Update and maintain executed delegation agreements to ensure that responsibilities of both the Alliance and the delegate as delineated under DHCS, DMHC, Knox-Keene Act, and/or NCQA requirements.
- Provide oversight of pre-delegation assessments or evaluations conducted by Alliance departments.
- Review of annual and/or focused ad-hoc delegation audit results and corrective action plans.
- Review and approve annual delegation calendar of audits.
- Review and analysis of contractual and regulatory reporting from delegated entities and subcontractors.
- Discuss operational and compliance issues for potential interventions (education, monitoring, corrective action, etc.).
- Review delegation and subcontractor performance dashboards including membership, utilization management, turnaround times, quality metrics, and encounter data scores.
- Oversee other delegated functions and/or activities with the intent of complying with regulatory and contractual requirements, including All Plan Letters (APLs).
- Implement interventions and/or recommend corrective actions as needed when opportunities for improvement are identified.
- Recommend revocation of delegation agreements, or contract termination if the delegated entity or subcontractor is

unable or unwilling to meet expectations despite appropriate interventions or requests for corrective actions.

- Ensure that significant delegation issues, activities, and risks are reported to Senior Leadership.

Reporting and Governance:

The SDOC shall meet on a quarterly basis, with ad-hoc meetings, if needed. Meeting minutes will be disseminated to its members and a summary will be presented to the Compliance Committee following each meeting. Meeting minutes must be reviewed for approval by the Committee at the following meeting. If a meeting cannot be held, the data and information from the previous meeting shall be disclosed at the next meeting of Committee members. The SDOC is not subject to Brown Act Requirements.

Appendix E

Administrative Oversight Committee Charter

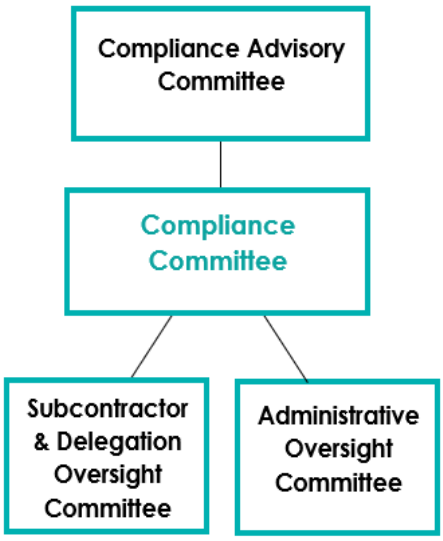
Purpose

The Administrative Oversight Committee (AOC) is responsible for facilitating the discussion and approval of administrative-related functions, processes, and other matters to ensure a streamlined and timely review. These may include:

- Policy and procedure review
- Risk and Issue Log review and remediation
- Key Performance Indicator (KPI) oversight and strategy adjustment
- Internal Audit Corrective Action Plan (CAP) review and closure approval

Committee Composition & Structure

The Chief Compliance and Privacy Officer (CCO/CPO) is the chair of the committee and shall provide leadership and oversight to the committee. The CCO/CPO may designate the Compliance Director as Chair or Co-Chair. The Committee's membership shall be comprised of senior subject matter experts and above from each department as determined by Senior Leadership Team (SLT) division leadership. Voting member count will be no less than fifteen (15) core members and no more than twenty (25). If a committee member cannot attend, they shall appoint a representative from their Department to attend in their place; this member must be named in writing via email and prepared as this representative will have voting power. For some actions and discussions, such as the review and approval of policies and procedures and risk and issue closure, a quorum of voting members must be in attendance. The quorum for AOC is a simple majority of voting members.



Meetings

The AOC will meet on a monthly basis (but no less than nine (9) times per calendar year. The Committee will meet less frequently, as necessary, depending on the number of topics needed for discussion, review, and approval at the discretion of Compliance.

Responsibilities and Functions

The functions of the Committee include the following actions:

1. Review and approve policies and procedures that further the goals and objectives of the Alliance's Code of Conduct and Compliance Program. Departments that make up the nine divisions will present their policies and procedures and explain any updates or changes.
    a. Policies and procedures may be approved via the PolicyTech Review and Approval Process, in certain situations, when a business need requires, outside of the regular cadence of AOC meetings.
2. Review and update Risk and Issue Log:
    a. Committee members and attendees will bring new risks and issues forward during and outside of committee meetings.
        i. All Alliance resources are capable of and encouraged to bring risk and issues forward in or outside of AOC committee.
        ii. Compliance and Internal Audit can initiate risks and issues at any time a deficiency is

noted without the business bringing the risk or issue forward.
    b. Committee members will vote on closure of all open risks and issues.
3. Review Key Performance Indicators (KPIs) related to compliance metrics and reported Dashboard metrics with a goal of ensuring Alliance operational health:
    a. Log Risks and Issues as necessary
    b. Monitor Risk and Issues to closure
4. Review Corrective Action Plans (CAPs) specific to the Compliance Department for Plan oversight, and vote to close any open CAPs in these areas.
5. Facilitate discussion of various administrative-related topics, and identify, suggest, or make necessary changes or updates to streamline the administrative affairs process and function.
6. Implement changes as necessary to further the Alliance's goals and objectives to align with internal and regulatory requirements.
7. Foster and guide the development of an efficient, effective, and clear discussion, review, and approval process for administrative functions, and the facilitation of this process.
8. Solicit quarterly feedback on the effectiveness of the Compliance Committee and its sub-committees through AOC meetings, anonymous surveys, and email. The feedback will be reviewed and used to make improvements on a continuous basis.

Reporting and Governance

Meeting minutes of the Administrative Oversight Committee must be approved by the Committee at the following meeting and maintained within the Compliance Department's dedicated AOC Teams Channel. The Administrative Oversight Committee summary of activities shall be reported to the Compliance Committee.

Appendix F

ALAMEDA Alliance FOR HEALTH

Health care you can count on.
Service you can trust.

ANTI-FRAUD PLAN

Table of Contents

I. BACKGROUND

Alameda Alliance for Health (Alliance) is a local, public, not-for-profit managed care health plan committed to making high-quality health care services accessible and affordable to Alameda County residents. We strive to improve the quality of life of our members and people throughout our diverse community by collaborating with our provider partners. The Alliance is honored to provide health care coverage for 2 out of every 10 Alameda County residents. We provide access to care and services to more than 400,000 people in our community. We partner with a network of more than 12,000 physicians and specialists, hospitals, and pharmacies to improve health outcomes and quality of life throughout our diverse community.

The Alliance is committed to preventing, detecting, and investigating fraud, waste, and abuse (FWA) incidents to protect our Alliance members and providers, and the integrity of the health plan. Through the adoption of the Alliance TRACK Values (Teamwork, Respect, Accountability, Commitment and compassion, and Knowledge & innovation), it is also the intent of the Alliance to comply with federal and state regulations, and contractual requirements concerning the detection, investigation, and resolution of suspected FWA.

The purpose of the Alliance Anti-Fraud Plan is to:

A.) Protect the Alliance's ability to deliver health care services to the Alliance membership through the timely detection, investigation, and prosecution of fraud.

B.) Develop and implement a process to protect the Alliance from internal fraud and from external fraud by providers, employees, members, and others.

C.) Provide various methods to report potential fraudulent activities to the appropriate authorities at the Alliance.

D.) Outline procedures for the detection, reporting, and managing of incidents of suspected fraud;

E.) 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;

F.) 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

G.) Educate the Alliance employees on applicable federal laws including the False Claims Act and whistleblower provisions.

II. ANTI-FRAUD ACTIVITIES

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

A. Structure

The Alliance's Chief Compliance Officer (CCO) is responsible for the Compliance Anti-Fraud Plan and activities. The CCO reports directly to the Chief Executive Officer (CEO), and to the Compliance Committee which oversees the Anti-Fraud activities. The Manager, Compliance Audits and Investigations, is responsible for the daily operations of the program and reports incidents and fraud prevention activity to the Compliance Director weekly, or more frequently if needed. The Compliance Director reports incidents and fraud prevention activity to the CCO at least monthly or more frequently if needed.

The Compliance Committee is comprised of senior leadership roles from each operational area of the Alliance. The Compliance Committee is responsible for reviewing and discussing the Alliance FWA 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 Alliance and discusses certain cases for resolution of any issues that arise. Any significant incidents are also reported immediately by the CCO to the CEO, and will be reported to the Board of Governors by the CEO or CCO.

The Alliance's Compliance Department works closely with internal departments on fraud detection process and investigations. These departments include Health Care Services, Provider Services, Member Services, Credentialing, Grievance and Appeals, Pharmacy, HealthCare Analytics, and Claims. Compliance 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,

pharmacy and medical utilization data analysis, clinical review of medical records, medical coder review, and monitoring of provider claims billing patterns.

B. FWA Reporting

The Alliance requires employees, contracted providers, and members to report any potential FWA incidents for investigation. All Alliance employees are required to promptly report all known or potentially fraudulent activities as explained in the Code of Conduct and Compliance trainings. If a supervisor or Human Resources receives a report of potential fraud, they will immediately notify the Compliance Department.

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

1) The Compliance Department mailbox at compliance@alamedaalliance.org;
2) Contacting any Compliance Department team member.
3) Directly to their Department Supervisor, Manager, or Director.
4) Contacting the Human Resources Department.
5) Calling the Compliance Hotline* at 844 587-0810; or
6) Submitting an online report via the Compliance Hotline link on the Alliance Intranet and external Alliance webpages.

   * The Compliance Hotline is a live twenty-four-hour-a-day telephone line and reporting website 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.

C. Regulatory Reporting

The 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. The Compliance Department maintains all FWA records and provides documentation as required and requested for external scheduled and ad-hoc reporting to appropriate state and federal law enforcement agencies. The Alliance strives to report all suspected incidents to DHCS within 10 working days. The Alliance will follow up on the incidents and provide DHCS with a case summary once the case is closed and will provide all investigation case documentation upon request.

D. Non-Retaliation Policy

It is the policy of the Alliance that no person shall be retaliated or discriminated against for reporting in good faith to the Alliance's CCO, the Alliance management staff, or to other proper authorities any alleged fraudulent activity committed by, on behalf of, or against the Alliance.

The False Claims Act (FCA) 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.

New Alliance employees are informed of the non-retaliation policy during the Compliance training and when reviewing and signing the Code of Conduct. The Compliance Department also annually provides training to all employees on the non-retaliation policy, and FCA and whistleblower provisions.

E. FWA Detection & Prevention

The Alliance strives to detect and prevent health care and insurance 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.

As required by 42 CFR §422.503(b)(4)(vi)(C) and 42 CFR §423.504(b)(4)(vi)(C), the Alliance implements a comprehensive Fraud, Waste, and Abuse (FWA) prevention and detection program. This includes mandatory FWA training for employees, contractors, and related entities, as well as self-reporting obligations to the Centers for Medicare & Medicaid Services (CMS) upon identification of any suspected FWA activities.

1) Fraud Data Detection

Provider claims data is routinely analyzed by the Compliance Department to detect any fraudulent activity. Data analyzed is specific to providers, facilities, members, medical services, and pharmaceutical services. The Compliance Department utilizes a vendor that reviews claims billing patterns within the last 12 months for providers and triggers claims found with suspected issues. The Compliance Department reviews the triggered suspected claims, and if valid will proceed with additional investigation which may include medical records review. This data analysis is critical for monitoring and identifying any repetitive fraud, waste, and abuse patterns. Over/under utilization, false claims, and unusual billing practices are also measures reviewed in the data analysis. Analysis findings are reported to the Compliance Director, CCO, and Compliance Committee.

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 the Alliance 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 drug utilization. From the reporting trends found, the Compliance Department will work closely with the Claims, Provider Relations, and Health Care Services 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

The Alliance conducts monthly exclusion screening of all providers of health care services or entities that contract with the Alliance 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 Medicare and Medi-Cal health care programs.

F. Investigation & Monitoring

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, recover funds paid as a result of fraudulent or wasteful payments, and work in collaboration with regulatory authorities and law enforcement. The investigator will conduct desk 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) in order 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. An investigation may consist of the following:

1) Documentation of allegation;
2) Comparing allegations to program policies and procedures;
3) Review of contract information;
4) Review of licensing and credentialing information;
5) Review of grievance and appeals information;
6) Review of medical records and authorization history;
7) Review of claims history;
8) Review of pharmacy authorizations and medication records;

9) Review of trends of prior allegations and/or reported incidents against provider;
10) Interview with the member/s, provider/s, and/or pharmacy/s involved;
11) Review by Medical Director;
12) Review by Legal Counsel; and
13) Determining type/s of corrective actions.

Corrective Action Plans (CAPs) and follow-up investigation plans are implemented, if applicable, to ensure any open issues and deficiencies are corrected. CAPs may include the following actions: medical record review, claims audit, provider education, provider claims monitoring, recoveries, and termination. Findings are reported to the CCO and to the Compliance Committee.

G. Education & Training

All Alliance employees are required to complete the Fraud, Waste, and Abuse Compliance training within 90 days of 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 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 those Alliance employees that do not meet the FWA training requirements, as described in policy CMP-026 Compliance Training and Education.

Providers receive FWA education and training materials through the Alliance online website. The online FWA educational materials are easily accessible and provide an overview of the importance of FWA detection, reporting, and prevention. The methods of reporting incidents and the Alliance's Compliance Department contact information are included in the online FWA materials. Delegated partners are annually audited for FWA

and compliance policies and procedures, training documentation, and reporting FWA incidents timely to the Alliance.

III. CONFIDENTIALITY OF THE ANTI-FRAUD PLAN

The Alliance has the responsibility to keep protected health information confidential in accordance with applicable federal and state laws. All FWA incidents reported, and investigations will remain confidential and shall comply with the Alliance HIPAA privacy guidelines and policies. The Alliance's Compliance Department will keep and maintain all records in compliance with State and Federal Retention guidelines.