Compliance Program Description

Issued by:
Commonwealth Care Alliance, Inc.
Corporate Compliance Department
Compliance Program Description
Reviewed and Revised November 2021

Table of Contents:

1. Introduction

Commonwealth Care Alliance, Inc. and its affiliates (collectively, “CCA”) are committed to conducting its business operations in compliance with ethical standards, internal policies and procedures, contractual obligations, all applicable federal and state statutes, regulations, and rules, including but not limited to, those pertaining to the Centers for Medicare and Medicaid Services (“CMS”) Part C and D programs, and the Health and Human Services Office of Inspector General (“OIG”). CCA’s compliance commitment extends to its internal business operations, as well as, its oversight and monitoring responsibilities related to its First Tier, Downstream and Related Entities and Medicaid Material Subcontractors (“FDR-MS”).

CCA formalized its compliance activities through a comprehensive Compliance Program. The Compliance Program incorporates the fundamental elements of an effective compliance program identified by 42 CFR 422.503(b)(4)(vi), 42 CFR 423.504(b)(4)(vi), 42 CFR 438.608, and the OIG and Department of Justice (“DOJ”) Federal Sentencing Guidelines.

CCA’s Compliance Program consists of the following regulatory and contractual focus:

- Corporate Compliance
- Health Plan Compliance
- Privacy and Security
- Internal Audit, Monitoring, and Corrective Action Plan
- Clinical Compliance
- Multi-State Contractual Compliance
- Fraud, Waste and Abuse

CCA’s Compliance Program contains the following core elements:

- Code of Conduct and Written Policies and Procedures
- Compliance Officer, Compliance Committee and High-Level Oversight
- Compliance Communications, Training, and Education
- Effective Lines of Communication
- Well Publicized Disciplinary Guidelines
- Systems for Routine Monitoring, Auditing, and Identification of Compliance Risks
- Prompt Response to Compliance Issues and Undertaking Corrective Action

CCA's Compliance Program is developed to:

- Promote compliance with all applicable federal and state laws and contractual obligations
- Prevent, detect, investigate, correct, and appropriately report suspected incidents of fraud, waste and abuse or program non-compliance
- Promote and enforce CCA's Code of Conduct
- Ensure member privacy requirements, including state and federal mandates
- Train and educate all Workforce and Board of Directors members on compliancetopics and their responsibilities concerning compliance
- Engage CCA's Executive Team, Workforce, Board of Directors, and FDRs, whenapplicable, in the Compliance Program.

2. Code of Conduct and Written Policies and Procedures

2.1 Code of Conduct

The Compliance Program Description enforces the mission of CCA's Code of Conduct, which serves as the organization's ethical and legal framework. All persons directly engagedin work on behalf of CCA, including all affiliates and subsidiaries, employees, temporary employees, volunteers, students, trainees, independent contractors, vendors or temporary employees ("Workforce"), and the Board of Directors ("Board") are expected to carry out their professional duties per CCA's Code of Conduct.

The Code of Conduct is reviewed annually by the Audit, Compliance, and Risk ManagementCommittee ("ACRM") of the Board and revised as necessary. The Board reviews and approves any significant changes to the Code of Conduct. The Code of Conduct is distributed to the Workforce and the Board at the time of hire, contract or appointment and as part of Annual Compliance Training. Workforce and the Board attest, on an annual basis, that they have reviewed the Code of Conduct. CCA's Code of Conduct is available to the Workforce through CCA's intranet, to the Board through the Board's portal, and the public, including members, providers and FDRs, on CCA's website.

The Code of Conduct includes, but is not limited to, the following topics:

- Compliance with the applicable federal and state laws, regulations, and Medicare and Medicaid program requirements
- Reporting Compliance Concerns
- Compliance Communications, Training and Education
- Cooperating with Audits and Investigations

- Conflicts of Interest
- Extending Business Courtesies
- Accuracy and Retention of Records
- Confidentiality of Member, Workforce and Business Information
- Fraud, Waste, and Abuse
- CCA's Non-Retaliation and Non-Intimidation Policy

2.2 Policies and Procedures

The Compliance Department maintains policies and procedures related to key compliance functions including, but not limited to:

- Fraud, Waste and Abuse
- Privacy and Information Security
- Regulatory Compliance Audits and Monitoring
- Compliance Communications, Training, and Education
- Investigating and Externally Reporting Compliance Concerns
- Compliance Risk Assessment
- Deficit Reduction Act, False Claims Act & Whistleblower protections, and
- Corrective Action Plans

All policies and procedures, including the history of updates, are found on CCA's governancetool, Cumulus. All CCA Workforce have access to the tool via CCA's intranet portal, CommonGround. Annually, CCA reviews its policies to stay current with contractual, legal and regulatory requirements. The Workforce and Board are required to comply with all applicable policies and procedures.

Key Compliance policies and procedures are distributed to the Workforce and Board members at the time of hire, contract or appointment and are accessible via intranet by the Workforce at any time. Policies are redistributed annually to applicable staff to ensure understanding, and adoption of the protocols outlined.

3. Compliance Officer and Compliance Committees

3.1 Chief Compliance Officer

CCA has a designated Chief Compliance Officer ("CCO") who is accountable to senior leadership. The CCO reports to the Chief Legal Officer and has a dotted-line reporting

relationship with the Board and CEO. This dotted-line relationship gives the CCO the authority to communicate directly with the CEO and Board of Directors, as necessary.

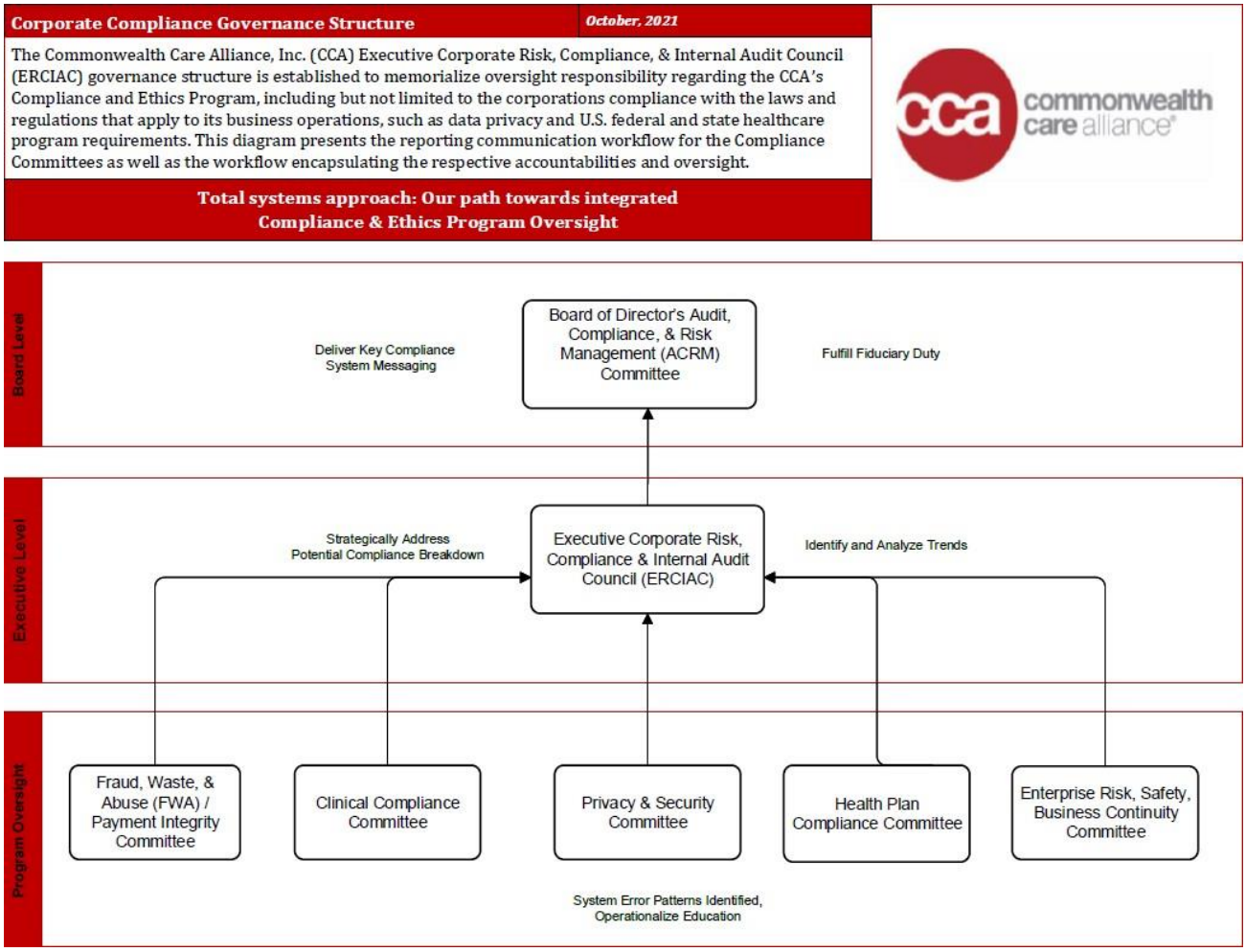
The Chief Compliance Officer is a full-time employee of CCA whose responsibilities include:

- Developing, enhancing, implementing and overseeing CCA's Compliance Program (Corporate Compliance; Health Plan Compliance; and Internal Audit).
- Developing, implementing and distributing the Code of Conduct as well as compliance-related Policies and Procedures to the Workforce, Board, and FDRsas appropriate.
- Implementing and maintaining the Compliance Training and Education Program that focuses on the Elements of an Effective Compliance Program (including Fraud, Waste and Abuse).
- Encouraging Workforce to timely report all suspected compliance concerns.
- Ensuring effective lines of communication are instituted and communication mechanisms are monitored, and complaints are investigated and treated confidentially to the extent possible.
- Ensuring inquiries and investigations of any reported or suspected compliance concerns are conducted timely and complete documentation is maintained. Outcomes of investigations are shared with leadership and the Board as required.
- Informing the Board of regulatory issues, trends, and risks.
- Overseeing Corrective Action Plans initiated by the Compliance Department as appropriate.
- Promoting a state of audit readiness for CMS, state agencies, state Medicaid programs, and other internal and external audits by distributing and monitoring updated protocols; and implementing best practices.

3.2 Compliance Department Organization Structure

Chief Compliance Officer		
Corporate Compliance	**Health Plan Compliance**	**Internal Audit**
Provides the core elements of the compliance program across all lines of business and all geographies. • Privacy & Security • Fraud, Waste & Abuse • Special Investigations Unit • Clinical Compliance Program • Compliance Education, Training, & Communications • Conflict of Interest Program • Incidents, Inquiry, & Investigations • Policies & Procedures • Overarching Compliance Plan, Risk Assessment, & Governance	Ensures compliance with contractual and programmatic requirements. Includes alignment with multiple geographies. • Regulatory (CMS, Medicaid, DOI) • Contract Compliance Monitoring • FDR Program (vendors)	Executes annual Internal Audit Workplan and manages internal and external audit findings to resolution. Provides support for the Enterprise Risk Management ("ERM") program. • Annual Internal Audit Workplan • Manage Regulator External Audits • Corrective Action Plans • SOC-2 & High Priority Controls • Key Risk Indicators (KRI's)

3.3 Compliance Committees*



*Implementation across CY21-22

3.4 Audit, Compliance and Risk Management ("ACRM") Committee

The Audit, Compliance and Risk Management ("ACRM") Committee was established by the Board to assist with fulfilling its oversight responsibilities concerning CCA's audit, compliance, and risk management programs. The ACRM Committee is made up of at least three members of CCA's Board of Directors and is staffed by the Chief Compliance Officer and Chief Legal Officer. This Committee assists the Board of Directors in fulfillingits oversight duties and oversees, among other things, CCA's Compliance Programeffectiveness, including but not limited to, compliance with regulatory requirements, laws, regulations, and compliance risks.

The ACRM Committee meets at least quarterly and receives reports on the activities and status of CCA's Compliance Program. The ACRM Committee provides regular reportsto the Board following each of its quarterly meetings. The Board is knowledgeable about the Compliance Program and its compliance

activities and is made aware of any potentialrisks.

The ACRM Committee's responsibilities include, but are not limited to:

- Be generally knowledgeable about health care compliance issues.
- Review the regular reports to management prepared by the Chief Compliance Officer, as well as management's responses to these reports.
- Oversee the organization's Compliance and Information Privacy and Security Programs to ensure effectiveness.
- Oversee the organization's compliance with legal and regulatory requirements.
- Annually review and recommend for approval to the board, the organization's Compliance Program for effectiveness per CMS and OIG requirements.
- Annually review and approve the organization's Information Privacy and Security Program, including HIPAA requirements.
- Oversee the organization's systems of disclosure of compliance concerns. The Committee should ensure that mechanisms are in place to ensure open communication among the Chief Compliance Officer, senior management, andthe Board of Directors.
- Oversee the organization's Code of Conduct and the organization's system to monitor compliance with and enforce this code.
- Annually review CCA's Code of Conduct and Conflicts of Interest policy and recommend any changes to the Board for approval.
- Oversee the performance of the Chief Compliance Officer and require prior approval by the Board of any action by the organization to discipline, suspend or terminate the Compliance Officer.
- Review the regular internal audit reports to management prepared by the Internal Auditor as well as management's responses to these reports.
- Oversee the organization's systems of disclosure controls and procedures, and internal controls over financial and operational reporting including any significant deficiencies and significant changes in internal controls. The Committee should encourage open communication among all independent auditors, senior management, the internal audit function, and the board of directors.

4. Compliance Training and Education Program

The Compliance Program outlines CCA's Compliance Training and Education Program. Workforce and Board members are trained on CCA's compliance policies, procedures

and regulatory requirements. Training materials are reviewed on an ongoing basis and updated appropriately to carry out the Compliance Program's mission.

4.1 New Employee Compliance Training

New Workforce members are assigned compliance training with completion due within ninety (90) days of their date of hire, contract or appointment. New Employee Orientation Compliance Training includes:

- An overview of general compliance topics; including the 7 elements of an effective compliance program to prevent, detect, and correct issues of non-compliance.
- Instructions on how to identify and timely report compliance concerns (including general compliance, Fraud, Waste, and Abuse ("FWA") or Privacy and Security concerns).
- Education about CCA's non-retaliation policy for reports made in good faith.
- Key Health Insurance Portability and Accountability Act ("HIPAA") and FWA principles, including a review of federal and state False Claims Acts, and whistleblower protections.
- An overview of the Physician Self-Referral or "Stark Law", Deficit Reduction Actand Anti-Kickback statute.
- Reviewing CCA's Code of Conduct.
- Instructions on how to identify and timely report compliance concerns.
- Review of compliance responsibilities for the Workforce.

Supplemental online courses are assigned and due for completion within ninety days of hire,contract, or appointment. This additional training includes:

Education on additional FWA regulations and scenarios.

- Code of Conduct
- Compliance Policies and Procedures
- HIPAA Privacy and Security review
- Reviewing and receiving key Compliance, FWA, and HIPAA Privacy and Security Policies and Procedures.

During these mandatory training activities, the Workforce becomes more familiar with CCA's Compliance Program and the role that compliance plays in their day-to-day job responsibilities.

4.2 First Tier, Downstream and Related Entity (FDR) and Material Subcontractor (MS) Training

CCA is contractually obligated to ensure that any individual or entity working on CCA's behalf to carry out CCA's duties will adhere to all applicable federal and state rules and regulations, including the Medicare Part C and D Programs, and for the dual-eligible programs, any applicable state Medicaid requirements. These are known as "FDR-MS" entities. Federal guidance requires that all FDR-MS entities involved with the administration or delivery of a Medicare or Medicaid benefit have access to general compliance and fraud, waste, and abuse training. CCA makes CMS' Medicare Parts C andD General Compliance and FWA trainings available on its website.

FDR-MSs who have met the certification requirements through enrollment into the Medicare Part A and B programs or through accreditation as a Durable Medical Equipment,Prosthetics, Orthotics and Supplies (DMEPOS) are deemed to have met the training and educational requirements. FDR-MSs who do not meet the deemed status are required to have staff working with CCA complete training that covers required topics (similar to CMS' General Compliance and FWA Training offered through the MLN network), including offering training themselves that meets requirements. CCA reserves the right to request and/or audit training documentation and records of completion.

Annual Compliance Training

The Compliance Department conducts Annual Compliance Training for all CCA Workforce and Board members, as a review of key compliance-related topics. Annual Compliance Training includes reviews of CCA's Code of Conduct, FWA, HIPAA, Privacy and Security, and the elements of an Effective Compliance Program.

Additional Methods of Compliance Training

Compliance Tips

The Compliance Department regularly distributes a "Compliance Tip" as an ongoing refresher on compliance-related topics via the company intranet, CommonGround.

Compliance Week

The Compliance Department conducts a Compliance Month to raise awareness ofrelevant compliance-related topics.

Direct Communication

CCA uses various methods of direct communication to notify the Workforce of any relevant federal and state regulatory changes, fraud alerts, pending changes to legislation, and advisory bulletins as necessary. The Workforce is continually advised on how additional compliance information can be obtained.

Documentation

All documentation related to trainings included in the Compliance Training and EducationProgram are maintained by the Compliance Department in accordance with CCA's RecordRetention Policy.

5. Effective Lines of Communication and Reporting

Open communication between the Compliance Department and CCA's Workforce, Board,and FDRs is a vital component of CCA's Compliance Program. CCA provides for routine,confidential and/or anonymous reporting of any compliance issues for all Workforce, plan members/patients, Board members, providers, vendors, and FDRs.

All Workforce is required to report, in good faith, any suspicion of non-compliant, unethical or illegal behavior. CCA Workforce is encouraged to discuss compliance-relatedissues directly with their managers/supervisors, with the members of the Compliance Department, or with the Chief Compliance Officer. However, in the event a person wishesto remain anonymous, they may use CCA's Compliance Hotline or Compliance Report e-Form on CCA's intranet, CommonGround under Compliance Connect. CCA publicizes the hotline number on posters within office locations, on CommonGround, on its website and in other communications, as appropriate. Reports are fully investigated, and summaries of reported compliance concerns may be shared with CCA's Senior Leadership and Audit, Compliance and Risk Management Committee as appropriate. Ultimately, all compliance-related concerns and outreach are centralized and managed through our Cumulus Inquiry and Incident (I&I) module. Below, outlines the ways, and parameters, in which Compliance can be outreached to:

Direct Reporting

CCA Workforce is encouraged to promptly report any compliance-related issues. They may contact the Chief Compliance Officer directly and/or use one of the other mechanisms provided.

CCA's Chief Compliance Officer:
James Moran.
617- 426-0600 x6991.
jmoran@commonwealthcare.org

Compliance Hotline

The toll-free 24/7 anonymous Compliance Hotline is available to report compliance-related concerns:

TOLL-FREE COMPLIANCE HOTLINE 1-866-457-4953

CommonGround

CCA has a company-wide intranet site called CommonGround which is accessible to all CCA Workforce. The home page of CommonGround showcases a section under Resourcesentitled "*Compliance Connect"* which houses key compliance-related documents such as instructions on how to report a Compliance concern, a Privacy and Security issue, or an FWA concern, as well as the Code of Conduct.

Compliance Incident Reporting

CCA offers an option for anyone to report Compliance Concerns via CCA's Governance, Risk and Compliance ("GRC") platform, Cumulus. This form allows any individual (both internal and external to the CCA Workforce) to report any compliance concern. A report can be submitted anonymously if the reporter chooses. These reports are automatically routed to the Chief Compliance Officer or his/her designee(s) for review and investigation. OtherCCA departments, as necessary, may be asked to participate in the investigation. The investigation notes, follow-up and final disposition are maintained within Cumulus.

Privacy and Security Reporting

Privacy and Security incidents are also managed within our Incident and Inquiry module within Cumulus. This form allows any individual (both internal and external to CCA Workforce) to report any privacy and/or security concerns. A report can be submitted anonymously if the reporter chooses. These reports are automatically routed to the Privacyand Security Officer or his/her designee(s) for review and investigation. Other CCA departments, as necessary, may be asked to participate in the investigation. The investigation notes, follow-up and final disposition are maintained within Cumulus.

Communication and Reporting Related to Fraud, Waste and Abuse-Internal Communication

The Compliance Department uses various methods to keep Workforce members informedof fraud, waste and abuse and their responsibilities under CCA's FWA. Topics related to fraud, waste and abuse are reviewed within the scope of the Compliance Training and Education Program.

Communication regarding FWA with Providers and Members

Providers and members are made aware of CCA's commitment to prevention, detection,identification and reporting of fraud, waste and abuse in the following manners: Provider Manual

CCA's external website
http://www.commonwealthcarealliance.org/ Periodic member

communications containing Compliance/FWA topics.

CCA also posts the Compliance Hotline number and Information about general complianceand Fraud, Waste and Abuse on its website http://www.commonwealthcarealliance.org/

Confidentiality and Non-Retaliation

CCA takes all reports of suspected violations and questionable conduct or practices seriously. Reports made to Workforce member's manager, Chief Compliance Officer, Compliance staff, the Compliance Hotline, or those submitted through CCA's intranet aretreated confidentially to the extent possible.

CCA prohibits any retaliatory action against a Workforce member for making a report in good faith. The Workforce shall not prevent or attempt to prevent another member of the Workforce from communicating a potential issue. Workforce members who attempt such action may be subject to disciplinary actions.

CCA's non-retaliation policy applies to good faith participation in CCA's compliance program, including, but not limited to reporting of potential issues, investigating issues,conducting self-evaluations, audits, remedial actions, participation in investigations andreporting to regulators and appropriate officials. CCA takes violations of this reporting policy seriously and the Chief Compliance Officer will review employee disciplinary and/or other corrective action for violations as appropriate with CCA's senior leadershipand the Board, as necessary.

6. Well Publicized Disciplinary Standards & Enforcement

CCA's Compliance Program includes the enforcement of standards through well-publicized disciplinary guidelines in the Code of Conduct. Any discipline in response to a violation of CCA's Compliance Program follows CCA's Employee Discipline Policy and Procedure.

The Workforce may be subject to disciplinary action for any compliance violation. Examples of conduct subject to enforcement and discipline include, but are not limited to:

- Failure to perform any required obligation relating to CCA's Compliance Program or applicable law;
- Failure to timely report, in good faith, any violations or suspected violations of the Compliance Program or applicable law;
- Failure to complete required Compliance training activities;
- A violation of CCA's Code of Conduct;

- Conduct that leads to the filing of a false or improper claim in violation of federal orstate law;

7. Effective System for Routine Monitoring, Auditing, and Identification of Compliance Risks

CCA has a system of ongoing compliance monitoring and auditing related to both its operations and the operations by contracted entities over which CCA has oversight responsibilities. The compliance risk assessment is a mechanism by which topics are selected for monitoring or auditing.

7.1 Compliance Monitoring

Departments conduct ongoing monitoring of activities performed within their department or by a contracted entity overseen by that department. Monitoring is the ongoing review of a department's own activities or their subcontractor's activities, collecting data and reviewing for a department's own understanding of timeliness, quantityof completion, and quality of completion.

Operational departments collaborate with the Compliance Department to identify monitoring reports that have a regulatory compliance component, based on risk assessmentand other factors. After establishing compliance monitoring reports, departments regularlyreview data for outliers and patterns to confirm and document ongoing compliance or to detect potential noncompliance. The Compliance Department reviews the summary reports for trends that indicate ongoing compliance or the potential for noncompliance and offers feedback to departments.

Specifically, CCA has developed the: Fraud, Waste and Abuse; Privacy & Security; Clinical Compliance and Health Plan Compliance Programs to prevent, detect, and correct issues of non-compliance and fraud, waste and/or abuse.

7.2 Fraud, Waste and Abuse Monitoring Activities:

- Routine monitoring of Workforce, providers, contractors and Board membersto identify and address individuals, entities or providers who have been excluded, precluded, or suspended from participating in federal and/or state health care programs.
- Creation and review of analyses to identify patterns and trends indicative of fraud, waste and abuse.
- Collaboration with internal departments, including Payment Integrity, Utilization Management, Claims, and Care Partnership.
- Oversight of and collaboration with FDR-MS entities.

- The **Fraud, Waste and Abuse Program Supplement** outlines the FWA efforts as they align with the seven core elements of an effective complianceprogram.

7.3 Privacy and Security Monitoring Activities:

- Assessments/audits to identify potential unauthorized or inappropriate access
- Workforce awareness of privacy policies and procedures
- Encouraging Workforce or member reporting
- The **Privacy and Security Program Supplement** outlines the privacy and security efforts as they align with the seven core elements of an effective compliance program.

7.4 Health Plan Compliance Monitoring Activities:

- Engages teams across CCA to review and attest to our contractual obligations under multiple health plan contracts.
- The **Health Plan Program Supplement** outlines the clinical compliance efforts as they align with the seven core elements of an effective complianceprogram.

7.5 Compliance Auditing

Internal Audits, including regulatory compliance audits, are conducted by the Compliance Internal Audit department. Internal Audits review compliance of processes performed by CCA departments or contracted entities, such as FDR-MSs. Internal Audits test and confirm compliance with Medicare and Medicaid regulations, sub-regulatory guidance, CCA's contractual obligations to the Centers for Medicare and Medicaid Services (CMS) and applicable Medicaid entities, applicable Federal and State laws, as well as CCA's internal policies and procedures.

The Annual Compliance Audit Plan outlines the planned list of audits, which are selectedthrough a variety of mechanisms, including risk assessment, monitoring results, and reports of potential noncompliance or FWA, FDR risk. Ad hoc audits not appearing on the AnnualCompliance Audit Plan may be performed when a high regulatory compliance risk is identified.

The commencement of Internal Audits may be announced or unannounced and the Compliance Department may use a combination of desk, virtual, and onsite audits. Appropriate and internationally accepted audit methods are used to determine methodology, including sample size, and auditors use statistically valid methods that comply with generally accepted auditing standards.

The Compliance Department approaches audits as a continuous improvement opportunity.Results are shared and impacted departments and entities are encouraged to

provide clarification before finalizing the audit report. Corrective action plans (CAPs) are requiredfor areas found to be non-compliant. Validation is conducted to determine if the implemented corrective actions have fully addressed the underlying problems. Audit results may prompt new or modified compliance monitoring reports.

Annual Compliance Risk Assessment

The Compliance Department facilitates and completes an annual compliance risk assessment. The compliance risk assessment process engages departments throughout CCA to identify and collect information about potential compliance risks. Risks resulting from internal processes, as well as risks to processes performed by FDRs overseen by CCA, are incorporated into the assessment. Identified compliance risks are ranked based on the potential impact and likelihood of a risk event occurring. The results of the compliance risk assessment are used to inform the CCA's Annual Compliance Plan, which includes the Compliance Auditing and Compliance Monitoring Plans.

Continuous Compliance Risk Assessment

The Compliance Department assesses potential compliance risks throughout the year to remain responsive to changes in CCA's operations, Medicare, Medicaid laws, regulations and requirements. The team works to identify and assess new (or previously unidentified) compliance risks, follow-up on previously identified compliance risks, and educate departments about accurately identifying compliance risks. New risks are analyzed using the same methodology as the annual compliance risk assessment process and may result in modification of CCA's Annual Compliance Plan or Compliance Auditing and Compliance Monitoring Plans.

8. Prompt Response to Compliance Issues and Undertaking Corrective Action

CCA's Compliance Program has procedures to ensure a prompt response to detected offenses and conducts a timely, reasonable inquiry upon discovery of evidence of misconduct; CCA develops and conducts appropriate corrective actions in response to identified violations. CCA makes every effort to correct problems promptly and thoroughly to reduce the potential for reoccurrence to ensure ongoing compliance withCMS and state agency requirements. When appropriate, CCA voluntarily self-discloses any potential misconduct to the appropriate external regulatory authority.

8.1 Corrective Action

CCA business owners and/or vendors work with the Compliance Department to develop compliance-related Corrective Action Plans ("CAPs"). A formal CAP is initiated when a noncompliance issue is brought to the attention of the Compliance Department through

an audit, monitoring, a department's or FDR's self-reporting, or through notification by CMS or state agency.

The CAP documents a process and completion of specific, tailored actions taken to achieve compliance with a specific requirement. The CAP process, which includes a root cause analysis, is designed to correct and mitigate the risk of recurrence of future noncompliance, as well as document the efforts taken to mitigate the noncompliant issue.

Reporting of Auditing, Monitoring, and Corrective Action Results

The Chief Compliance Officer receives regular summary reports of all audit, monitoring, and corrective action activities and provides select updates to the Internal Compliance Committee, CCA's Senior Leadership and the ACRM Committee who makes regular reports to the Board. CCA may also disclose an issue to the appropriate regulatory agency.

8.2 Disclosing Issues to Regulatory Bodies

The Compliance Department maintains a structured decision-making process to determine if an identified issue should be formally disclosed to CCA's CMS and/or state agency Account Manager. Representatives from the Compliance Department, internal business departments and/or the Legal department may be involved in the decision-making process.

8.3 Notice of Violation or Suspected Violation

The Workforce is required to promptly and in good faith, report a violation, suspected violation; questionable or ethical conduct in violation of the Compliance Program and/or Code of Conduct, or applicable law to his/her supervisor/manager, the Chief Compliance Officer, through one of CCA's reporting mechanisms. When a report is received, it is promptly investigated and resolved as soon as possible.

8.4 Response to Notice of Violation or Suspected Violation

After an investigation is complete, the Chief Compliance Officer or his/her designee notifies applicable senior leadership and/or the Audit, Compliance and Risk Management Committee, as appropriate to determine a proper response.

The investigation and risk mitigation activities may include some or all the following:

- Investigating all aspects of the suspected violation or questionable conduct.
- If the investigation involves Part C or D potential misconduct, a referral to a Medicare Integrity Contractor ("MEDIC") will be made based upon reportingrequirements for MEDIC reports, including follow-up filing for preliminary reports.
- If CCA conducts an inquiry that is determined to be potential fraud, waste or abuse or misconduct, CCA will refer the misconduct to the appropriate regulatory authority timely, including the MEDIC, state, or federal agencies, as appropriate.

- When appropriate, CCA will prepare a Corrective Action Plan to address and correct the misconduct to mitigate the risk for repeated misconduct.
- When appropriate, CCA will provide refresher education on the area identified in the misconduct.

Response and Resolution Related to Fraud, Waste and Abuse ("FWA")

Any suspected cases of fraud, waste or abuse that are to be reported to the Department of Regulatory Affairs and Compliance are sent to CCA's Special Investigative Unit (SIU) to lead the investigation. After investigation, if an FWA incident is determined to have occurred, appropriate action will be taken. Appropriate action may include:

- Referral of any abuse or potentially fraudulent conduct for further investigation toCMS and/or the MEDIC concerning Medicare activities; to the state Attorney General's Office in relation to Medicaid activities; including any entities as appropriate.
- Prompt reporting of potential violations of state and federal law to the appropriatelaw enforcement authorities.
- Disciplinary actions up to and including termination of any Workforce who engages in fraudulent or abusive practices; and potential contract termination for any contracted entity found to have conducted any misconduct.
- When appropriate, CCA will prepare a Corrective Action Plan to address, educate, correct and monitor the misconduct in order to mitigate the risk for repeated misconduct.
- When appropriate, CCA's SIU will recommend new or modified controls, policies, procedures, and/or processes to the business to prevent, mitigate and reduce identified risks in the future.
- Also, when appropriate, CCA will provide refresher training on the area identified in the misconduct.

9. Fraud Waste and Abuse Program Supplement: Program Overview

9.1 Policy Statement

All CCA Workforce members, contracted providers, First Tier, Downstream and Related Entities (FDRs), business associates, and delegated entities are obligated to report any suspicion of fraud, waste and abuse in a timely manner. Internal and external reporting

mechanisms are available to anyone who suspects fraud, waste or abuse within CCA or its network.

9.2 Program Mission, and Goals

The mission of CCA's Fraud, Waste and Abuse Program is to protect the integrity of CCA,along with federal and state programs, by detecting, preventing, investigating and reportingsuspected cases of fraud, waste and/or abuse.

The goals of CCA's Fraud, Waste and Abuse Program are to:

- Detect, prevent, investigate, and report incidents of fraud, waste, and abuse;
- Recommend and implement internal policies, controls, and procedures including monitoring and reviewing trends to access risk and mitigate forrecurrence;
- Report instances of substantiated fraud, waste, or abuse to the appropriategovernment agencies and/or law enforcement;
- Cooperate fully with all investigations of fraud, waste or abuse conducted bygovernment agencies and/or law enforcement;
- Recover payments lost to fraudulent, wasteful and/or abusive billings;
- Provide communication and education regarding fraud, waste and abuse;
- Educate CCA Workforce and other entities, as required, on how to identifyfraud, waste, and abuse;
- Provide methods for internal and external individuals to report suspectedincidents of fraud, waste, or abuse;
- Communicate on a frequent and timely basis to the business any adverse provider action, suspensions, and terminations and manage member impact, asappropriate.

Fraud, Waste and Abuse Program Organizational Structure

9.3 Senior Leadership

The development and ongoing monitoring of the FWA Program is charged to the CorporateCompliance Department, overseen by the Chief Compliance Officer (CCO). The roles and responsibilities listed below include specific functions related to fraud, waste and abuse androutine operational activities that may contribute to the detection, prevention, investigation and reporting of fraud, waste and abuse.

Contact information for the Chief Compliance Officer is as follows:

James Moran
Chief Compliance Officer
Commonwealth Care Alliance

30 Winter St., 11th Floor Boston, MA 02108
Phone: 617-426-0600 Ext. 6991
Email: jmoran@commonwealthcare.org

9.4 FWA Committee

CCA's cross-functional Fraud, Waste, and Abuse Committee meets at least quarterly to provide guidance and oversight to the FWA Program. The FWA Committee consists of representatives from multiple departments including Business Intelligence, Claims, ClinicalServices, Dental Services, Finance, Legal, Member Services, Pharmacy, Provider Contracting, Provider Relations, and Transportation Services.

9.5 Special Investigations Unit

CCA's Special Investigations Unit (SIU) supports the Chief Compliance Officer in preventing, detecting, investigating, and reporting all suspected, potential or confirmed fraud, waste, and abuse to the appropriate state or federal and regulatory entity and worksin cooperation with state and federal regulatory and/or law enforcement agencies in investigations of suspected fraud, waste, and abuse as necessary.

CCA's SIU staff serve as the subject matter experts regarding health care fraud, waste, andabuse. Along with developing and maintaining SIU systems and processes, they are also responsible for providing leadership and direction regarding fraud, waste, and abuse to internal and external entities.

The FWA Program & SIU Manager is responsible for the daily program operations andstaff investigations and reporting activity. SIU Investigators and Analysts report to the FWA Program & SIU Manager.

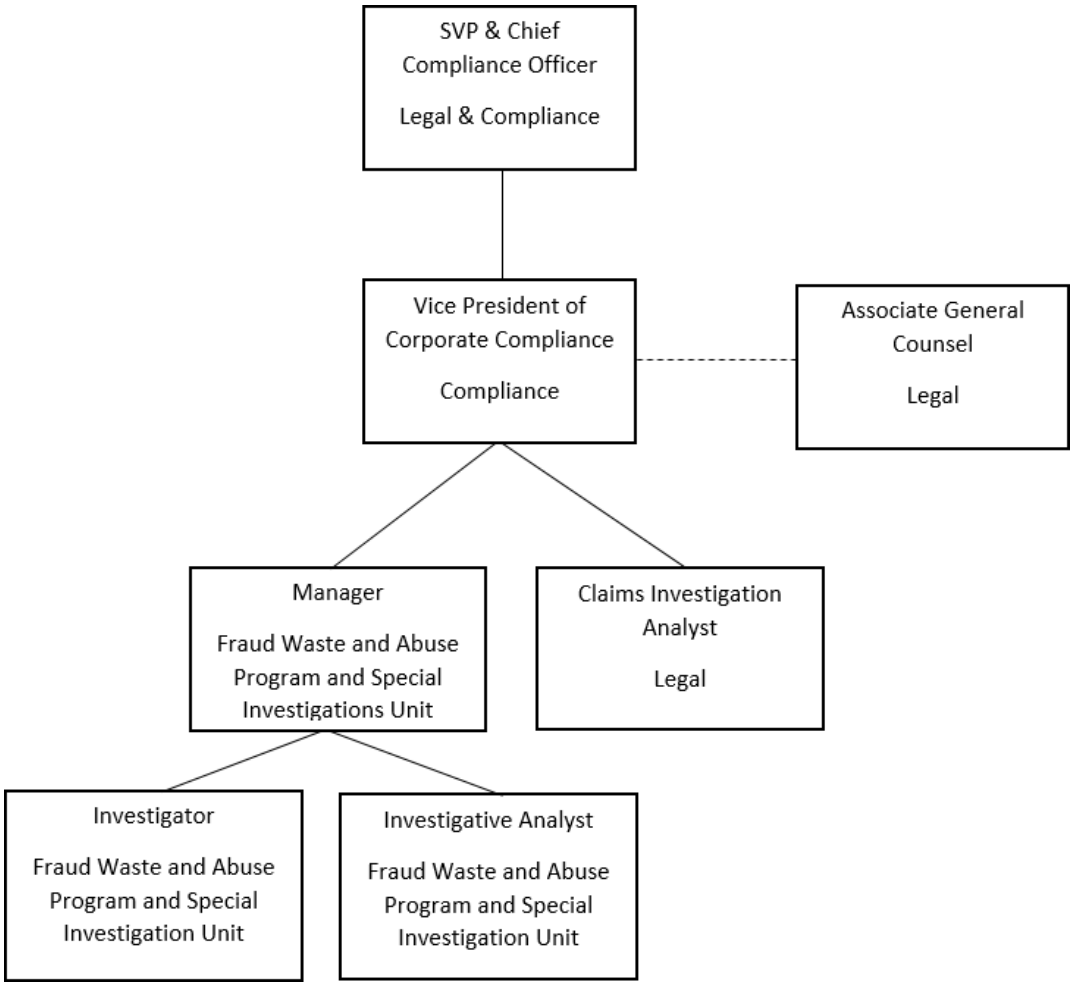
CCA contracts with the Navitus Pharmacy Benefit Manager for SIU services relating to CCA's pharmacy benefits. CCA's internal FWA Program & SIU meets quarterly with theNavitus team and assists Navitus with member and medical investigations involving pharmacy-related issues.

The Legal Department within CCA supports the efforts and activities of CCA's FWAProgram & SIU.

- Responsibilities of the FWA Program & SIU include, but are not limited to:
- Leading a cross-functional Fraud, Waste and Abuse Committee;

- Developing policies and procedures to a) prevent fraud, waste and abuse and b)assure internal controls are in place to address risk areas;
- Monitoring and researching laws and regulations impacting CCA's FWA Program;
- Investigating reported cases of suspected fraud, waste and abuse;
- Reporting all substantiated cases of FWA to appropriate external agencies;
- Maintaining documentation of all investigations;
- Conducting ongoing fraud, waste and abuse training;
- Researching all fraud alerts issued by CMS, OIG or the Massachusetts AttorneyGeneral to determine the impact to CCA;
- Providing FWA training materials to members and contracted entities;
- Annually reviewing the FWA Program Description.

9.6 SIU Organizational Structure



FWA Program: Confidential Reporting of Suspected FWA

9.7 Reporting Suspected FWA

All Workforce, FDRs, and contracted partners are required to report, in good faith, any suspicion of fraud, waste or abuse in a timely manner. CCA makes available multiple different methods for reporting suspected non-compliance, including methods that allow the reporter to remain anonymous.

Direct Reporting

Anyone who suspects fraud, waste or abuse may contact the FWA Program & SIU directlyat FWA_Team@Commonwealthcare.org.

Reports may also be made directly to the CCA Chief Compliance Officer by mail, email, orphone:

James Moran
Chief Compliance Officer Commonwealth Care Alliance 30 Winter St., 11th Floor Boston, MA 02108
Phone: 617-426-0600 Ext. 6991
Email: jmoran@commonwealthcare.org

CCA Workforce may also report concerns directly to their supervisors, who should then useany of the reporting mechanisms listed here to report the concern to the Corporate Compliance Department.

CCA maintains a toll-free, 24/7 Compliance Hotline:

TOLL-FREE COMPLIANCE HOTLINE1-866-457-4953

Reports made to the Compliance Hotline may be made anonymously. CCA posts the Compliance Hotline number on its website as well as on the CCA intranet, CommonGround.

CCA offers an option to report fraud, waste and abuse concerns via its Governance, RiskManagement, and Compliance platform, Cumulus (also called Compliance360):

Cumulus Compliance Concern Report Form:

https://secure.compliance360.com/ext/M8F8EwSrYFo=

This form allows any individual (both internal and external to the CCA Workforce) to reportany compliance concern, including suspected fraud, waste or abuse. A report can be submitted anonymously if the reporter chooses. These reports are reviewed by the Compliance department and then routed to the appropriate unit based on the allegations.

FWA SharePoint:

CCA Workforce members with access to the CCA shared network may also submit concerns using the FWA Sharepoint form, which is accessible through the Compliance page of CommonGround. Concerns reported using this form are sent directly to the SIU. The FWA Sharepoint form can be found at: https://commonground.commonwealthcare.org/CF/CII/FWAI/SitePages/FWA%20Incident s.aspx

9.8 Confidentiality

CCA takes all reports of suspected violations and questionable conduct or practices seriously. All information received or discovered by the SIU will be treated as confidential,and the results of investigations will be discussed only with persons having a legitimate reason to receive the information. Individuals who wish to report their concerns anonymously may do so using theCompliance Hotline.

FWA Program: Education and Awareness

9.9 Workforce

As part of the FWA Program, CCA's SIU supports the Corporate Compliance Departmentin developing and providing training to Workforce members regarding the recognition, detection, prevention, and reporting of suspected fraud, waste, and abuse. Training is provided within ninety (90) days of the date of hire, as part of the annual Compliance Training and Education Program, and on an ad-hoc basis as required.

Topics covered within the FWA training and education include, but are not limited to:

- Definitions of fraud, waste and abuse.
- Examples of fraud, waste and abuse.
- Review of specific industry scenarios and current schemes.
- Current CCA practices to detect, prevent, and report fraud, waste and abuse.
- Review of key regulations concerning FWA including, but not limited to:
    - Deficit Reduction Act
    - False Claims Act (Federal and State)
    - Whistleblower Protections (Federal and State)
    - Anti-Kickback Statute
    - Stark Law
    - Civil monetary penalties of the Social Security Act

- Fraud and Abuse, Privacy and Security Provisions of the Health InsurancePortability and Accountability Act, as modified by HITECH Act
- Fraud Enforcement and Recovery Act of 2009
- Patient Protection and Affordable Care Act

In addition, CCA maintains a written Code of Conduct which addresses CCA's commitment to addressing instances of non-compliance. The Code of Conduct is made available to all Workforce via the CCA Intranet, CommonGround, and is also available to external partners via the Provider Manual.

CCA's Corporate Compliance Department, with support from the SIU, uses various methods to keep Workforce members informed of fraud, waste and abuse and their responsibilities under CCA's Fraud, Waste and Abuse Program. The Corporate ComplianceDepartment will periodically issue Fraud Alerts on CommonGround, CCA's external website, or within member or provider communications to educate the Workforce, FDRs and members on special or pressing concerns relating to fraud, waste or abuse.

9.10 FDRs and Providers

CCA's contracts include language requiring compliance with all applicable policies, federaland state laws and regulations, including the Medicare Part C and D Programs and state Medicaid requirements. Federal guidance requires that all entities involved with the administration or delivery of the Medicare benefit have access to general compliance and fraud, waste, and abuse training. CCA makes CMS' Medicare Parts C and D Fraud, Waste and Abuse Training, and Medicare Parts C and D General Compliance Training available to FDRs and providers on its website.

FDRs who have met the certification requirements through enrollment into the Medicare Part A and B programs or through accreditation as a Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) are deemed to have met the training and educational requirements. FDRs who do not meet the deemed status are required to have staff working with CCA complete training that covers required topics (like CMS' General Compliance and FWA Training offered through the MLN network). CCA reserves the rightto periodically request and/or audit training documentation and records of completion.

CCA makes information about fraud, waste and abuse available to providers and FDRs via information contained in CCA's Provider Manual, on the external CCA website, and withinperiodic provider communications.

9.11 Members

Members are made aware of CCA's commitment to prevention, detection, identificationand reporting of fraud, waste and abuse, and how they can report allegations for investigation, via CCA's member enrollment documents, external website, and periodicmember communications containing Compliance/FWA topics or alerts.

FWA Program: Prevention and Detection

9.12 Routine Operational Activities

CCA utilizes various routine operational activities throughout normal business operations which may result in the prevention or discovery of potential fraud,waste and/or abuse.

9.13 Contracts

CCA includes language in its contracts with providers, vendors, and other FDRs requiring those entities to abide by all applicable laws, rules, regulations and policies. Contracts also include language requiring that entities comply with applicable federal and state requirements for Workforce trainings, including anti-fraud, waste, and abuse training for all employees. Provider contracts specify entities may not employ or contract with any individual who is or has ever been excluded from the Medicaid or Medicare programs.

Additionally, provider contracts give CCA, CMS, or other delegated entities the right to conduct audits of provider records and services and requires that providers comply in a timely manner to any audit requests from those entities.

9.14 Credentialing

CCA's credentialing process is designed to ensure that contracted providers are appropriately credentialed in alignment with standards promulgated by the National Committee for Quality Assurance (NCQA), Centers for Medicare and Medicaid Services (CMS), and relevant state regulations, including EOHHS.

CCA credentials providers prior to admitting the provider into CCA's network, and periodically thereafter. CCA maintains a Credentialing Committee which reviews concerns identified during the credentialing process and considers and votes on the appropriateness of providers' continued participation in CCA's network based on credentialing findings.

9.15 Suspended, Excluded, and Precluded Lists

CCA routinely checks state and federal suspension, preclusion, and exclusion lists to

ensure CCA does not knowingly employ, contract with, and/or make payments to entities that are barred from receiving state and/or federal funds. CCA works closely with its vendors to periodically review claims data to ensure any claims submitted by suspended, precluded, or excluded entities are appropriately adjudicated based on the provider's status.

9.16 FWA Prevention and Detection Activities

CCA's SIU engages in various activities specifically designed to prevent and detect possible fraud, waste or abuse concerns.

9.17 Risk Analysis

CCA's SIU conducts quarterly risk assessments to identify and prioritize concerns which may increase CCA's risk of potential fraud, waste and abuse. The results of this risk assessment are incorporated into the FWA Program work plan, which guides the SIU's annual activities and goals.

9.18 Data Analytics

Data analysis may be used to identify aberrant service patterns, potential areas of overutilization or underutilization, changes in provider or member behaviors, and possibleimproper billing schemes. CCA's SIU may utilize data analysis to establish baseline benchmarking data, enabling the SIU to recognize unusual trends, changes in utilization, and/or schemes to inappropriately maximize reimbursement. The SIU works closely with the Business Intelligence team to develop tools to identify trends indicative of potential fraud, waste or abuse.

9.19 Monitoring of Media and Industry Communications

CCA's SIU monitors news and media outlets daily for information relating to fraud, waste,or abuse risks which may affect CCA or CCA members. The SIU utilizes automatic alerts to search local and national media for press releases, arrests, indictments, settlements, or other news related to fraudulent or improper activity by providers or related entities. The SIU also monitors for bankruptcies, facility closures, lawsuits, complaints, or other activitywhich may impact CCA or its members. The SIU may open investigations or conduct audits in response to media alerts. Additionally, the SIU monitors for alerts or communications from leaders in the compliance and anti-fraud industries, which may provide information or guidance relatingto local or national fraud, waste or abuse trends.

9.20 Fraud Alerts and Notifications

CMS, OIG, and the DOJ, among others, periodically release special fraud alerts or bulletinsto make plans and providers aware of schemes or trends impacting the

healthcare industry. CCA's SIU closely monitors these alerts and responds as instructed by conducting data analysis, opening investigations, and/or performing other control activities in response to these notifications.

9.21 Cross-Functional Collaborations

CCA's SIU works closely with several internal and external stakeholders to identify and address concerns related to fraud, waste and abuse. The SIU routinely meets with vendors,such as CCA's Pharmacy Benefit Manager and Transportation Benefit Manager, to assessand support their anti-fraud activities and to evaluate waste prevention mechanisms. The SIU collaborates with these vendors to detect, investigate, and resolve potential cases of fraud, waste or abuse.

The SIU also collaborates with internal stakeholders to improve internal controls and identify trends indicating potential fraud, waste or abuse. For example, the SIU works closely with the Utilization Management department to identify and respond to concerns related to the over- or underutilization of services by members or providers.

Members of CCA's SIU are actively involved with the anti-fraud industry and meet regularly with regulators, law enforcement, and related entities to discuss current trends, risks, and opportunities.

9.22 Claims Edits

CCA utilizes industry-standard edits to identify and deny instances of improper billing and to identify and address services billed that require a review of supporting documents before payment.

9.23 Payment Policies

CCA uses payment policies to communicate the requirements needed for CCA to reimbursea provider for services. CCA's Payment Policy Committee is a cross-functional group that identifies, prioritizes, researches, prepares, and votes on new and updated payment policies.CCA's payment policies can be found on CCA's external-facing website.

Response to Allegations of Potential FWA

9.24 Policies and Procedures

CCA develops and maintains policies and procedures to ensure prompt reporting and response to potential fraud, waste, and abuse. CCA maintains processes for reviewing, approving, and updating policies and procedures as required.

9.25 Investigations

CCA makes every effort to investigate and correct problems promptly and thoroughly to reduce the potential for reoccurrence to ensure ongoing compliance with all applicable requirements. As part of CCA's Fraud, Waste, and Abuse Program, the SIU is responsiblefor conducting reasonable, timely investigations into allegations of potential fraud, waste,or abuse. The purpose of an investigation is to gather evidence related to an allegation to determine the likelihood that potential fraud, waste, or abuse may have occurred. If an allegation is substantiated, the SIU may conduct further investigation or analysis to determine the scope and impact of the non-compliance and to quantify and recover any associated overpayments.

CCA's SIU may investigate allegations lodged against providers, members, vendors, CCAWorkforce, and/or any other related entity involved in CCA's business operations.

9.26 Investigative Process

Concerns reported to the SIU are investigated promptly, with preliminary investigation activity beginning not more than two weeks after the date the concern was reported. Every investigation is unique, and the scope of the investigation is defined by the specifics of each allegation.

Upon receipt of an allegation of potential fraud, waste, or abuse, CCA's SIU will conduct apreliminary investigation to determine the likelihood of improper behavior and the impact of that behavior if substantiated. Preliminary investigations may include, but are not limitedto, data analysis, open-source research, review of prior allegations or investigations if present, regulatory and policy research to determine if what is alleged is a violation, interview(s) with the complainant to obtain further information, and/or review of internally maintained records.

If the preliminary investigation determines the activity did not occur, was not a violation ofpolicy or regulation, did not result in a financial loss to CCA or related entities, or has an otherwise reasonable explanation based on fact, CCA will document the findings, close thereferral, and will not pursue further investigation. If the preliminary investigation determines the allegation is not an FWA matter, the SIU will refer the allegation to the appropriate internal department.

If the preliminary investigation identifies suspicious activity, a more extensive investigationmay be conducted. This may include but is not limited to: statistical sampling; record requests and reviews; interviews with the Workforce, members, vendors, providers, or witnesses; data analysis; on-site inspections; and/or other investigative activity intended to substantiate or quantify fraud, waste or abuse.

The SIU documents the investigative steps and findings within its case management systemand maintains these records for a minimum of ten (10) years following the

completion of a review.

9.27 Cooperation with Audits and Investigations

All CCA Workforce, vendors, FDRs, providers, and their employees are obligated to cooperate with all audits or investigations performed by CCA, CMS or its delegated contractors, law enforcement, or other regulatory body with authority to audit or investigateCCA's business practices and those of its contractors. Failure to cooperate with reasonable requests related to audits or investigations may result in disciplinary action, up to and including termination of employment or contracts with CCA, and the recovery or reversalof associated claim payments.

9.28 Attorney-Client Privilege

Where applicable, CCA's SIU applies appropriate procedures to maintain attorney-client privilege in matters involving the advice of CCA's legal counsel. The SIU marks privilegedcommunications appropriately and restricts access to privileged records or information.

9.29 Reporting Credible or Substantiated Allegations of FWA

CCA promptly reports any credible allegations or substantiated instances of fraud, waste, orabuse to the appropriate internal departments, regulatory bodies, and/or law enforcement entities as appropriate.

Reports may be made by mail, phone, email, or via a dedicated complaint form on an official agency website. Reports may include, but are not limited to, information regardingthe target of the investigation, the allegation and allegation source (unless complainant chooses to remain anonymous), the nature of the alleged behavior, a summary of evidencegathered throughout the investigation, and an estimate of damages resulting from the non-compliant behavior.

CCA's SIU may make reports to any or all of the following entities, dependent on the specific circumstances of the situation:

- Health and Human Services Office of the Inspector General (HHS-OIG)
- U.S. Department of Justice (DOJ)
- The Centers for Medicare and Medicaid Services (CMS), or its delegated entities responsible for program integrity such as the Medicare Drug Integrity Contractor(MEDIC)
- State Medicaid agencies
- Medicaid Fraud Control Units
- Social Security Agency

- Local law enforcement

This is not a comprehensive list, and the SIU is responsible for identifying the appropriate entity to which concerns of fraud, waste, or abuse should be reported. Additionally, the SIU may make reports to the Compliance Committee(s), Chief Compliance Officer, or other internal stakeholders as necessary.

9.30 Corrective Action

When incidents of fraud, waste, abuse, or other non-compliant activity are identified, CCAworks to promptly institute corrective actions to mitigate future losses and reduce the risk of recurrence.

Corrective actions may include, but are not limited to:

- Clinical intervention and education.
- Issuing warning letters or notices.
- Providing or requiring education or training.
- Revising policies or procedures.
- Instituting internal controls such as claims edits or document reviewrequirements.
- Suspension of payment during investigations or audits.
- Termination of employment or contracts.
- Recovery of overpayments.

When appropriate, CCA will develop a formal Corrective Action Plan (CAP) to address, educate, correct, and monitor entities found to have engaged in misconduct.

CCA's SIU regularly makes recommendations for additional controls, policies, procedures,and processes CCA or its contracted entities may implement to reduce, prevent, and detect fraud waste and abuse.

9.31 Ongoing Monitoring

CCA conducts ongoing monitoring of entities found to have been involved in fraudulent, wasteful, or abusive practices. Continued non-compliance will result in termination of employment or contracts, where appropriate.

10. Privacy & Security Program Supplement: Program Overview

10.1 Program Mission and Goals

Commonwealth Care Alliance, Inc. and its affiliates (collectively, "CCA"), in conformity

with the Compliance Program Description, has developed a Privacy and Security Program to oversee and monitor compliance with state and federal laws and regulations applicable to the privacy and security of personal health information and protected data. The mission of CCA's Privacy and Security Program is to uphold a culture of privacy and security compliance that strengthens and further demonstrates CCA's commitment to appropriately safeguarding the privacy of an individual's health information and protected data.

10.2 Goals and Objectives

The overarching goal of the Privacy and Security Program is to provide a structure that promotes understanding and compliance with the HIPAA Privacy and Security Rules, related provisions of the HITECH Act and applicable state privacy and security laws, thereby ensuring that the affairs of the organization are conducted per laws, regulations, contractual obligations, and guidelines applicable to such activities.

Specifically, the goals and objectives of the Program are as follows:

1. Establish policies and procedures to promote compliance with applicable federal, state, and local laws, regulations and ordinances.
2. Outline organizational and departmental compliance roles.
3. Establish mechanisms to implement CCA's Privacy and Security Program, which includes:
    - Conducting regular assessments of current uses of secured data and protected information as well as the corresponding policies and procedures to identify areas requiring greater safeguards and oversight.
    - Developing and implementing ongoing training, including the creation and dissemination of policies and procedures, to ensure that CCA Workforce members and external partners are aware of any legal requirements and/or contractual obligations and are updated promptly on any changes in the standards or policies.
    - Developing and implementing a means for CCA Workforce members and external partners to raise questions and concerns of non-compliance and receive responsive guidance as appropriate.
    - Documenting Privacy and Security compliance efforts and providing reports of such efforts, including complaints, investigations and reporting incidents to the appropriate oversight bodies and leadership.
    - Establishing a mechanism for individuals to report instances of non-compliance, so such reports can be fully investigated.
    - Formulating corrective action plans to address any issues of non-

compliancewith Privacy and Security policies and standards.

- Coordinating compliance efforts with external partners and other interested parties.

Privacy and Security: Roles and Responsibilities

10.3 Privacy and Security Officer

CCA shall designate an individual to serve as its Privacy and Security Officer. CCA's Privacy and Security Officer shall oversee compliance efforts with guidance from the Privacy and Security Compliance Committee and in collaboration with CCA's Information Security and Compliance teams. The Privacy and Security Officer is accountable to the VicePresident of Corporate Compliance.

The Privacy and Security Officer chairs the Committee and coordinates implementation and ongoing compliance efforts company-wide. Key responsibilities include:

- Overseeing, monitoring and coordinating the CCA Privacy and Security Program.
- Identifying and assessing security risks to personal information and systems.
- Developing policies and procedures for the protection of confidential information.
- Facilitating input and approval of privacy policies, Compliance Program Descriptions and other materials with the advice of the Privacy and Security Committee and VP of Corporate Compliance.
- Coordinating privacy and security compliance efforts, including education and training.
- Monitoring and assessing CCA's external partners and suppliers.
- Responding to and facilitating the resolution of breaches and complaints.
- Ensuring incident response and disaster recovery plans are developed and implemented.

10.4 Privacy and Security Committee

The CCA Privacy and Security Committee ("Committee") serves in an advisory role for the overarching Privacy and Security Program to promote appropriate information handling practices and risk-based safeguards that protect individually identifiable health information. The Committee operates under the auspices of the Vice President of Corporate Compliance.The Committee, chaired by the Privacy and Security Officer, was implemented to address CCA's obligations to comply with the HIPAA Privacy and Security

regulations. Responsibilities of the Committee include:

- Advising the Privacy and Security Officers on HIPAA requirements as needed.
- Assisting the Privacy and Security Officer with the promotion and accomplishment of CCA's Privacy and Security Program and related compliance efforts.
- Reviewing, providing input and approving HIPAA policies, procedures, compliance plans and other CCA compliance program artifacts.

The Privacy and Security Committee includes representatives from the following departments:

- Privacy and Security Officer
- Legal / General Council
- Clinical Services
- Health Plan Operations
- Information Security

The Privacy and Security Committee represents a subset of individuals on the Corporate Compliance Committee and Information Security Working Group.

Representatives from this Committee may bring matters forward for approval or acceptance by the VP of Corporate Compliance, as necessary. In addition, representatives from the Committee may be convened to provide guidance regarding urgent matters (*e.g.*, a data breach or complaint) at the discretion of the Privacy and Security Officer or Vice President of Corporate Compliance.

10.5 Coordination with External Partners

The Privacy and Security Officer is responsible for coordinating with external partners to:

- Align policies and procedures and expectations.
- Foster a community based upon trust and safeguarding PHI.
- Assure those with access to secure data and protected information are appropriately trained.
- Coordinate breach and security incident response(s).

Key external partners include, but are not limited to:

- Health Homes
- Long-Term Support Services (LTSS)

- Third-party suppliers (where applicable)

Privacy & Security Program: Framework

10.6 Policies and Procedures

The Privacy and Security program has developed a set of policies and procedures to addresscompany compliance with the privacy and security requirements.

10.7 Education and Training

CCA's Privacy and Security Officer will be responsible for coordinating and implementing education and training to ensure policies and expectations are disseminated and understood.The training and education provided by the Privacy and Security Officer (or designate) mayinclude:

- Resources, such as a self-assessment checklist, to aid Workforce members in assessing and maintaining compliance.
- Assisting Workforce members in reviewing assessment results and developing policies and procedures to address identified compliance issues and mitigate potential risks.
- Assisting with questions and providing information related to policies and procedures.
- Communicating about changes to privacy and security rules.
- How to report potential security incidents or breaches.

Privacy & Security Program Auditing and Monitoring

The Privacy and Security Officer will work with Internal Audit and Information Security to identify and prioritize the relevant scopes of compliance reviews. Audits will be conducted as routine, by special request or as part of corrective action. If a review identifies issues of non-compliance, the Privacy and Security Officer will work with the appropriate Workforce member to rectify the issue(s). If necessary, The Privacy and Security Officer may consult General Counsel or with the Committee to determine if there has been any activity inconsistent with law or company policy. If, at the conclusion of any review, it appears there are compliance concerns, a corrective action Program Description will be formulated and initiated on a timely basis.

10.8 Audit Process

Audits may be initiated for just cause following breaches, complaints or suspected non-

compliance as well as on a routine basis. Audits shall be conducted following the audit procedures established by the Privacy and Security Officer.

Audits may include the following:

- Review of the policies and procedures and other related documentation related to compliance with Privacy and Security Rules.
- Review of the security risk assessment and remediation Program Descriptions.
- The assessment of administrative, physical & technical safeguards including the assessment of the security of the physical site and safeguards for systems used to store, retrieve or share PHI.
- Assessment of training compliance.
- Assessment of privacy and security risks.

10.9 Risk Analysis

The Privacy and Security Officer will regularly conduct general risk assessments to identifyfocus areas for auditing purposes. The Privacy and Security Officer will then work with Internal Audit to prioritize audits and to develop the audit schedule.

Privacy & Security Program Reporting Systems &Corrective Action Initiatives

CCA Workforce members are both encouraged and required to report any activity believed to violate this Program Description or any legal requirements to one or more of the following:

Contact the Compliance Team directly at CCA Compliance
CCA_Compliance@commonwealthcare.org

Reports may also be made directly to the CCA Chief Compliance Officer by mail, email, or phone:

James Moran
Chief Compliance Officer Commonwealth Care Alliance 30 Winter St., 11th Floor
Boston, MA 02108
Phone: 617-426-0600 Ext. 6991
Email: jmoran@commonwealthcare.org

CCA maintains a toll-free, 24/7 Compliance Hotline:

TOLL-FREE COMPLIANCE HOTLINE 1-866-457-4953

(Reports to the Compliance Hotline may be made anonymously.)

Cumulus Compliance Concern Report Form:
https://secure.compliance360.com/ext/M8F8EwSrYFo=

This form allows any individual (both internal and external to the CCA Workforce) to report anycompliance concern. A report can be submitted anonymously if the reporter chooses. These reports are reviewed by the Compliance department and then routed to the appropriate unit.

10.10 Investigations

Matters reported are to be directed to the CCA Privacy and Security Officer and investigated promptly to determine their veracity. Whenever a compliance issue has been identified, the Privacy and Security Officer shall notify the appropriate parties and seek guidance as needed. There may also be consultation with the appropriate directors, liaisons or CCA Workforce. The CCA Privacy and Security Officer or their designee shall maintaina log that records, reports the nature of any investigation and its results.

Failure to report knowledge of wrongdoing may result in disciplinary action. Any manager receiving a report of possible non-compliance must immediately advise CCA's Privacy and Security Officer.

10.11 Corrective Action Plans

Corrective action may require changes to information handling and data protection practices, development or changes in policies and procedures, completion of training and other efforts to mitigate risks to privacy and security of Protected Health Information (PHI). Sanctions or discipline, in accordance with company policies, may be recommended. The Privacy and Security Officer has the responsibility and authority to take or direct appropriate action. The Privacy and Security Officers will prepare a recommended corrective action Plan as appropriate. A record will be maintained of any reports. Each complaint will be investigated. After a review and investigation, the Privacy and Security Officer will prepare a written report of findings and identify any corrective action that is required.

10.12 Open Lines of Communication

CCA will not retaliate against any individual who reports actual or suspected violations of the laws, regulations, or policies. All reported violations will be handled with the utmost integrity to ensure the confidentiality of the identity of the reporting individual and the person or persons involved in a suspected violation.

11. Health Plan Compliance Program Supplement: Program Overview

The Health Plan program of Commonwealth Care Alliance, Inc. and its affiliates

(collectively, “CCA”) oversees eight core programs and processes. The CCA drives compliance with regulatory and contractual laws, regulations and requirements. Foundational contentstems from the Contract Compliance Program, which measures how effectively we are meeting contractual and product requirements, and where our key areas for developmentlie. Our first tier, downstream, and related entities program ensure vendor compliance with regulatory requirements prior to contracting and throughout the contract relationship. The department’s monitoring processes ensure ongoing oversight and escalation around gaps and risks highlighted through the Health Plan programs.

Where internal and external parties have compliance-related topics to raise, the Compliance Incidents & Inquiries process centralizes intake and ensures timely resolution by the subject matter expert on the given topic. Additionally, the Health Plan Program manages notifications and directives via a memo from either federal or state entities to ensure affected departments have adopted the given directives timely and in their entirety. CCA’s Health Plan Compliance department serves as a contact for member or operational concerns raised by the State, or State entities, and as a guardrail for timely and accurate responses and implementations.

As CCA continues to expand its products and renew existing contracts, Compliance is regularly playing a key role in ensuring overall readiness in that evaluation, be it external or internal. The Compliance team supports readiness in these efforts by identifying key business owners, content collection and evaluation, and identifying risk areas.

In all areas, programs have measures regularly collected and analyzed to identify trends in risk areas, development bottlenecks, and effectiveness in the management of our programs to drive insights and results for our departments’ objectives. Lastly, the Health Plan Compliance Committee has been chartered to monitor overall health plans’ compliance with regulatory and contractual laws, regulations and requirements, and, the effectiveness of the overall Health Plan Program, outlined within.

11.1 Contract Compliance Program

CCA’s Compliance team manages a comprehensive inventory of contractual responsibilities across our SCO, One Care, MAPD, and DSNP products. The Contract Compliance Program evaluates compliance with responsibilities to confirm the degree to which CCA meaningfully meets each requirement. CCA manages adherence to its contractual and product requirements via its Contract Compliance Module (CCM), housed within Cumulus, CCA’s internal Regulatory Affairsand Compliance database.

For each unique component, a record has been assigned to a given business owner within the department associated with the scope of work described. The business owner has attested to a current level of compliance and continues to do so annually, each fall. This ensures CCA can always confirm the current level of compliance with a given contractual requirement, as a department, and company-wide. This enables CCA to have insights into

any of the areas of open development, as it pertains to effectively demonstrating howCCA meets the requirement. These insights, where significant, can lead to future strategic initiatives for ongoing improvement.

Where full compliance has been attested to, business owners have been asked to provide supporting documentation to demonstrate how CCA has met the requirement. Examples of common documentation types are a policy, workflow, DST (decision support tool), RG (reference guides), SOP (Standard Operating Procedure), Job Aid, or Workflow. Where a given requirement states submission of a report or hitting a target metric, the record ideally holds the most recent example of that report or data set. Compliance reviews all documentation to confirm it meaningfully demonstrates how CCA fulfills therequirement and engages with the business owner where documentation does not capture the full scope of work stated.

CCM's portfolio of documentation will foster preparation for cross-functional documentation exercises, such as EQRs, readiness assessments, and new product launches.The database is also a general search tool to identify a given department's key scopes of work and main contacts when inquiries arise.

Where there are gaps in compliance, business owners have been asked to state what developments are needed, and how they can be achieved. This exercise also highlights any obstacles to improvement within the department. The goal is to ensure we know where there may be risks and encourage feasible improvements. Within each record, the business owner has documented milestones for improvement. This enables Compliance to work with the business owners throughout the year, ensuring we make progress to close gaps.

The annual attestation period ends with both high-level, and detailed summary reports being provided to each SVP at each year-end. The reports capture their departmental and business owner-specific compliance levels, highlight key areas of improvement, and act as an overall assessment on how the department is meeting the expectations of our contractual and product requirements. This ensures a 3-way understanding across Compliance, business owners, and senior leadership.

Beyond the fall attestation and documentation period, Compliance monitors any not-fully compliant records throughout the remainder of the year, reviewing the business owners' progress at hitting milestones and meeting with business owners where there may be obstacles to development.

Contract Compliance metrics are presented both annually, and monthly, to highlight progress, and core areas of development. CCM can generate reports to show any at-risk areas by the business owner and department, both in terms of compliance levels and, timely engagement in the monitoring workflow.

11.2 Health Plan Compliance: FDR Program

CCA maintains a comprehensive scope of activities to oversee vendors, including first tier, downstream, and related entities (FDRs), and Medicaid Material Subcontractors (MS) as applied to the Medicaid portion of H0137 and H2225. CCA is responsible for fulfilling the terms and conditions of contracts with CMS, and state agencies, such as, theExecutive Office of Health and Human Services (EOHHS) offices, and is, therefore, accountable for vendor compliance with Medicare program requirements.

FDRs require a heightened level of oversight due to the nature of the contracted services performed on behalf of CCA, the impact on members, and the level of decision-making authority granted by CCA to FDRs.

Operational business owners are responsible for identifying the need for a vendor to perform work on behalf of CCA, evaluating the vendor's ability to perform contracted activities through regular oversight. Business owners are responsible for understanding and adhering to Medicare and Medicaid program requirements that pertain to their operational functions and are also responsible for reporting potential issues of non-compliance, suspected privacy or security concerns and/or potential incidents of fraud, waste, and abuse to the CCA Compliance Department. Compliance works with business owners and assists in outreach with business owners to compliance staff at their FDR-MS entities when appropriate.

CCA has processes in place to promote and verify vendor compliance with regulatory requirements prior to contracting and throughout the contract relationship. The Compliance Department is responsible for maintaining an effective compliance program, which includes oversight of vendors, with a particular focus on FDR-MS entities. Compliance has a role in certain oversight activities, including first tier entity determination, educating business owners about their responsibilities for FDR oversight, maintaining records of offshore entities within HPMS, exclusion list screening of vendors, education and contract review of vendors regarding the need to exclusion checktheir own staff and engagements, distributing compliance information and training, FDR-specific risk assessments, compliance monitoring, compliance auditing, investigating potential issues of reported non-compliance, potential fraud, waste, and abuse, potential privacy and security incidents, overseeing regulatory compliance corrective actions, and reporting issues as appropriate to Compliance leadership and/or organizational leadership.

11.3 Review Process for FDR-MS Entities

CCA maintains a collaborative review process that involves multiple teams assessing new contracts. As part of the review process, Compliance's FDR Program Manager, and/or their designee reviews the vendor against set criteria to determine if the vendor should be designated as an FDR. Broadly, the three main factors are:

1. Whether the entity is performing Medicare or Medicaid contractual duties.
2. Whether the entity has access to members or member's PHI.
3. Whether CCA is gatekeeping the entity's actions or is delegating decision-making.

As part of the initial review process, exclusion database checking and assessing offshoreaccess are also reviewed. If the entity meets the criteria for an FDR, then the FDR Questionnaire, FDR Attestation, and (if necessary) the offshore downstream disclosure form is sent to the entity.

When entities are flagged as an FDR, the review process issues the Medicare Advantage/Medicaid Managed Care Appendix as part of their contract. The FDR Questionnaire assesses whether the entity has a compliance program. These include but are not limited to obtaining validation from the vendor that they have a process to review exclusion databases upon hire, contract and appointment; and monthly thereafter, has policies and procedures around effective communication, reporting of and investigating incidents as well as suspected cases of FWA or HIPAA breaches, and clarifying whether the entity has been reviewed by third-party auditors to validate its program. Regulatory Affairs teams work jointly to review entities' responses, and each reserves the right to request additional information. If the vendor meets the requirements, the entity is cleared to proceed. Compliance then engages the business owner around expected monitoring for both business needs and continued compliance program effectiveness of the entity. Entity review team includes:

- Procurement
- Finance
- Legal Affairs
- Health Plan Compliance
- Privacy & Security
- Information Technology (IT)
- Business Unit (Department) that will directly oversee the operations of the contractor

11.4 FDR-MS Methodology

CCA's procedure for determining first tier entities is based upon the definition and guidance provided by CMS in Section 40: Sponsor Accountability for the Oversight of FDRs of Chapter 21 – Compliance Program Guidelines of the Medicare Managed Care Manual and Chapter 9 - Compliance Program Guidelines of the Prescription Drug Benefit Manual, 42 CFR 422.504, 42 CFR 438.2, as well as industry and historical guidance. The below is taken directly from CCA's SOP on First Tier Entity determination.

Medicare Advantage/Part-D First Tier Entity Analysis: An entity contracted to provide services on behalf of CCA is an MAPD First Tier Entity if ***all three*** of the following questions are answered YES:

Q1. Does the function (to be) performed by the entity appear on any of the followingthree CMS lists of functions that impact CCA's Medicare contract with CMS? (See CMS List of Functions Impacting CCA's Medicare Contract)

- Material Provisions of an MA Contract (Material) – MMCM Chapter 11, Section 100.1 Medicare Advantage Plan Core Functions (Core) – MMCM Chapter 11, Section 100.5
- Functions related to Medicare Part C and D contracts (Related) – MMCM Chapter 21/ PDP Chapter 9, Section 40

Q2. Does the function (to be) performed by the entity affect members ("Affect" means any of the following three questions answered "Yes")?

- Directly impact members?
- Interaction with members (in-person, verbal, or written)?
- Access to PI or PHI?

Q3A or Q3B: *Either of these*

Q3A: Does the entity have decision-making authority for the function (impacting CCA's Medicare contract with CMS)?

- Yes - Decision-making – Definition: "Monitor and Sample": The entity has decision-making if the business grants the vendor the right to execute the Medicare or Medicaid function on its behalf without gatekeeping, and CCA only monitors and reviews the work the vendor is performing, then the vendor has decision-making authority.
    - Example: Pharmacy benefit manager (PBM). Executes a large portion of the Medicare Part D functions. CCA monitors their contract requirements, such as pharmacy appeals, formulary management/rebates, and maintains the pharmacy network contracts. They require PHI to process claims and maintain membership drug interactions. The PBM does not request CCA to review and approve of every decision; thus, the PBM has been delegated decision-making to act on CCA's behalf in all the above functions.
    - Consultants providing advice-and-counsel services, where the advice is generally meant to be confidential and not for disclosure short of a court order, are not considered FDRs so long as CCA has actual and 100% reviewed final implementation decision. E.g., contract lawyers,

auditors, etc.

- Instances where CCA is substituting or filling in a lack of skill or knowledge via consultants are not automatically exempt and require evaluation against whether gatekeeping is present in their oversight. E.g., Workforce augmentation, like hiring consultants to perform MDS assessments due to CCA needing additional staff to meet deadlines
- **No Decision-making**–The entity does not have decision-making power,therefore is ***not*** an FDR. CCA acts as a gatekeeper, and the contractor cannot proceed without each Medicare or Medicaid contract item beingpermissioned by CCA. If this would negatively impact the vendor's ability todo business, then it is a delegated decision-making.
- Example: Mail and print vendor. Executes part of the member communication function per the Medicare and Medicaid contract and uses PHI to do so. However, it only prints exactly what CCA orderswhen CCA orders it.

Q3B: Is the entity in a position to commit FWA due to: the function they will be doing, the ability to harm members, or the capacity to violate Medicare program requirements (regulations, laws, guidance, etc.)?

Medicaid-only Material Subcontractor Analysis

An entity contracted to provide services on behalf of CCA is a Medicaid-only FTE if the following questions are answered YES:

Q1. Would the entity qualify as a First-Tier **except** it is primarily, or only, for Medicaid or other non-Medicare services? (Note that behavioral health care coordination is considered Medicaid focused due to Medicaid's higher priority than Medicare for BH needs)

Q2: Is it an entity other than a network provider OR it is a network provider who is performing services that fall under plan administration or healthcare services (e.g., care coordination, care planning) outside similar providers of the same category?

If Yes to Q1 and Q2, follow the same protocols as FTE "Yes" result for a Medicaid Material Subcontractor. If not, identify as a non-material subcontractor, and send offshore attestation only if PHI is involved. As noted in the diagram, above, Medicaid-only entitiesare not First Tiers but are instead Medicaid Material Subcontractors and are handled similarly. Downstream entities are evaluated using the same methodology.

11.5 First Tier Risk Assessment

A focused first tier entity risk assessment is performed periodically. The first-tier entity risk assessment is distinct from the administrative vendor/consultant risk analysis. The first-

tier entity risk assessment includes information captured directly from annual first tier entity compliance attestations, compliance monitoring and auditing, and CCA's contract management software systems. The following items are considered in the risk assessment:

- Function/service performed
- Member access - in-person, direct, indirect
- Downstream entities
- Offshore PHI access, either of the First Tier or a downstream
- Regulatory requirements placed on function
- Nature of the function positioning entity to potentially commit FWA
- Authority granted to an entity to make decisions
- Impact on and interaction with CCA Members
- Level of access and use to PHI
- CCA's compliance experience with the entity (e.g., attestation, prior audit results)
- Whether or not the entity is already queued for the internal audit plan due to FDR Attestation responses

Each first-tier entity is accorded a point value based on the information outlined above, and first tier entities are ranked in order of priority for compliance activities. Business owner input and activities, collected via the Annual Compliance Risk Assessment, monitoring, routine discussions with Compliance, audit results, and other data collection methods, are also factored into the risk level for each first-tier entity. Overall regulatory priorities, including regulatory guidance, are considered when determining the first-tier entity's individual risk level.

Based on the results of the first-tier entity risk assessment, Compliance may initiate one or more of the following actions for a selection of first tier entities identified as priority risks. These are presented to the Internal Audit team for consideration of adding the entityto the year's audit plan:

- Request supporting materials from the first-tier entity.
- Work with the business owner to confirm understanding of oversight responsibilities.
- Work with the business owner to incorporate additional or enhanced monitoring.
- Conduct a compliance audit of the first-tier entity.
- Other actions or projects tailored as necessary.

CCA has further enhanced the FDR monitoring program to require the issuance of data and reports demonstrating compliance with compliance program effectiveness measures from business owners, beginning in 2021. These focus on recurring, high-risk items, specifically exclusion checking results, disclosure of incidents/logging that incidents were disclosed during the month if already disclosed, and quarterly and annual measures to assess training requirements. Incident disclosure includes reporting, responding to, and taking corrective action when issues are found across the universe of potential compliance issues. When an issue is uncovered, this is evaluated in the frame of whether it constitutes a compliance concern or an operational concern. This monitoring also includes the capture of business SLAs (service level agreements) that define why CCA is using the business, frequently being related to the portion of the federal contract which CCA delegated to the entity.

11.6 Health Plan Compliance Program: Monitoring

CCA conducts routine compliance monitoring of activities performed by CCA departments and by FDRs. Topics are identified for compliance monitoring through several mechanisms, such as the annual and FDR risk assessments, reports of suspected non-compliance or FWA, and Audit results. Priority topics per CMS, EOHHS, and other applicable regulators are also key components of CCA's monitoring.

Compliance Monitoring is conducted by a Monitor within the Internal Audit, Compliance, FWA or Privacy and Security Units. The Monitor works with key departmental business owners to identify metrics within their departments that tie to a compliance requirement. After establishing the metrics and reporting, compliance threshold(s), and frequency of the reporting, departments conduct ongoing compliance monitoring activities that include regularly reviewing data for outliers and patterns to confirm and document ongoing compliance or to detect potential noncompliance or FWA.

Departments submit compliance monitoring summary reports to the Monitor, in order to identify any trends, or obstacles to improve where needed. Monitor references result from compliance monitoring reports to prepare for related audits and to analyze risks during the compliance risk assessment.

Overall trends are discussed at Health Plan Compliance Committee (detailed below). Here, the Committee can assist with and advise on appropriate strategies or approaches to improve operational or programmatic risks identified through our monitoring program.

11.7 Health Plan: Compliance Incidents & Inquiries

CCA's Workforce and members of the Board of Directors are encouraged to report any compliance concerns including suspected cases of fraud, waste and abuse. We also encourage providers and members to report concerns. A CCA Workforce member who, in good faith reports a concern, is not subject to any form of retaliation or retribution. To

the extent possible, confidentiality is maintained in every investigation.

Compliance inquiries and concerns may be reported in several ways: verbally to a manager, Chief Compliance Officer, or on the Compliance Hotline; web-based submissions, through CCA's electronic reporting system Cumulus, accessible through the Compliance page of CCA's intranet - CommonGround; through the FWA reporting form, accessible through the Compliance page of CCA's intranet; via email to the FWA or Compliance inboxes.

Once an inquiry is assigned based on type, topic, and area of expertise, the investigator may consult with others such as Compliance staff, Chief Legal Officer, senior leadership, or the Board of Directors, as appropriate. Cases of suspected Fraud, Waste and Abuse are directed to CCA's Special Investigative Unit for investigation. Issues identified as not compliance in nature (e.g., Quality of Care concern; member grievance) are directed to the appropriate internal department for investigation.

Depending on the incident or inquiry, a concern may be reported to an agency, such as: Centers for Medicare and Medicaid Services ("CMS"), state-specific External Office of Health and Human Services ("EOHHS") agencies, or the Attorney General's Office Medicaid Fraud Division ("MFD"). CCA's Leadership, Board Audit, Compliance and Risk Management Committee, and/or Fraud, Waste and Abuse Committee are informed of substantiated instances that are externally reported.

A thorough investigation of each case is completed and documented within Cumulus and becomes part of the overall metrics, to highlight areas of incident, inquiry, as well as themes around resolution.

11.8 Health Plan: Product Readiness

Compliance participates in preparing both our own, and external departments in effectively demonstrating regulatory and contractual readiness for our various products, including SCO, One Care, D-SNP, and MAPD product lines. These readiness exercises include both pre-launch to the public, or, in support of an external evaluation, such as a state evaluation in advance of a contractual extension.

For state evaluations, Compliance works with the business and PMO to leverage existing knowledge and content regarding business ownership, documentation, and potential gap areas across our various databases, such as CCM and Policy. The goal is to create efficiencies in data collection, as well as consistency in the vetted documentation we use to externally demonstrate how our operations meet contractual and regulatory obligations. Compliance reviews documentation for clarity, depth, and accuracy prior to external dissemination.

Product readiness for the DSNPs also includes the annual SMAC submission (State Medicaid Agency Contract). This exercise confirms and itemizes to CMS where our State

contracts meet the specified Federal expectations. Compliance works with the State EOHHS to amend our contract as needed each year, to accommodate any new parameters presented by CMS. Compliance also engages with departments affected by any new regulations that need to be incorporated into CCA's operations or standards.

For a new product launch, Compliance staff identifies core regulatory requirements each department should consider in preparing their area to accommodate the new product specifications. Requirements are discussed with each department to highlight where new business processes need to be developed. All new business requirements are added to the CCM module to track and ensure readiness progress is demonstrated in advance of the product go-live within the market. High-risk items critical to product launch are highlighted and prioritized.

11.9 Health Plan State Engagements and Escalation

CCA's Health Plan Compliance department serves as a contact for member or operational concerns raised by the State, or State entities, such as the Ombudsman. The team serves as a guard rail, focusing on timely and accurate responses for escalated member concerns raisedexternally. Compliance is represented on the State's product-specific monthly calls (SCO &One Care) to ensure any high-level risks are disseminated, if raised.

11.10 Regulatory Memoranda and Requirements Monitoring

Compliance staff reviews all incoming state and federal regulatory memos to ensure affecteddepartments have adopted the given directives, both timely, and in their entirety. State memosmay include formally published notices, provider bulletins, or state executive actions. Examples of federal memos include those from CMS, the Federal Register, or the OIG.

Applicable memos are assigned via our Regulatory Memoranda and Requirements Monitoring module to key business owners within a department for review and implementation where applicable. Compliance reviews business owner feedback, and ensures any memos with a confirmed implementation need, receive confirmation from the business on how that has been achieved.

Additionally, within this program is compliance management for ongoing or ad hoc reporting requirements that refer largely to state and federal entities. Business owners are engaged viathe module to generate the required data, submit it to Compliance for review, meet timely submission requirements, and collect the associated documentation.

The regulatory memo and requirement program measures timeliness for regulatory memo adoption and required reporting submission. This enables any risks to be highlighted from memos needing leadership support to drive adoption.

11.11 Health Plan Compliance Committee

The Health Plan Compliance Committee was formed to represent and assist the Executive Corporate Risk, Compliance, & Internal Audit Council ("ERCIAC") in fulfilling its oversight responsibility regarding the Corporation's Compliance and Ethics program, including but not limited to its compliance with the laws and regulations that apply to its business operations, U.S. federal and state healthcare program requirements and contractual compliance. The Committee coordinates with both the ERCIAC and the Board's Audit Compliance & Risk Management Committee ("ACRM") in monitoring health plan compliance with regulatory and contractual laws, regulations, and requirements.

The members represent cross-functional leadership across business and clinical departments, each providing their unique insights on significant operational risk areas related to compliance, and the steps management has taken to monitor, control, and report such risk exposures. The committee monitors the effectiveness of CCA's Health Plan Compliance Program and recommends improvements as necessary or appropriate, including the effectiveness of the system for monitoring health plan compliance with relevant laws, regulations, and government policies

Additionally, the findings of internal/external audits and corrective action plans, and large-scale policy changes from state and federal regulators are discussed in order to ensure effective implementation.

12. Definitions Glossary

Abuse- Describes actions that are inconsistent with sound fiscal, business, or medical practices that may, directly orindirectly, result in: unnecessary costs to any health care benefit program, improper payment, payment for services that fail to meet professionally recognized standards of care,or medically unnecessary services. Abuse involves payment for items or services when there is no legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment. Abuse cannot be differentiated categorically from fraud because the distinction between "fraud" and "abuse" depends on specific facts and circumstances, intent and prior knowledge, and available evidence among other factors.

CMS Centers for Medicare and Medicaid Services: Federal agency under the Department of Health and HumanServices responsible for administering the Medicare andMedicaid programs.

Department of Justice (DOJ)- The United States Department of Justice, also known as the Justice Department, is a federal executive department of the United States government tasked with the enforcement of federal law and administration of justice in the

United States.

D-SNP- Dual Eligible Special Needs Plans (D-SNPs) enroll individuals who are entitled to both Medicare (title XVIII) and medical assistance from a state plan under Medicaid (title XIX).

Downstream Entities- A party that enters into a written arrangement, acceptable to CMS EOHHS with persons or entities involved with a Medicare Part C, or Part D benefit, below the level of the arrangement between Commonwealth Care Alliance and a first-tier entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services.

ERM- Enterprise risk management (ERM) is the process of methodically identifying and addressing the potential events that represent risks to the achievement of strategic objectives.

FCA False Claims Act- is a federal law that imposes liability onpersons and companies who defraud governmental programs. It is the federal Government's primary tool in combating fraud against the Government.

FDR- First Tier, Downstream, and Related Entities.

First Tier Entity- A party that enters into a written arrangement, acceptable to

CMS, with CCA to provide administrative services or health care services to a CCA member for Medicare Part Cand/or Part D benefits.

Fraud- Knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program or to obtain (through false or fraudulent pretenses, representations, or promises) any ofthe money or property owned by, or under the custody orcontrol of, any health care benefit program.

HPMS- Health Plan Management System is CMS' web-enabledinformation system that serves a critical role in the ongoingoperations of the Medicare Advantage (MA), Part D and MMP programs. HPMS functionality facilitates the numerous data collection and reporting activities mandatedfor these entities by legislation. HPMS also provides support for the ongoing operations of the plan enrollment and plan compliance business functions.

LEIE- List of Excluded Individuals and Entities: OIG's List of Excluded Individuals/Entities (LEIE) provides information to the health care industry, patients and the public regarding individuals and entities currently excluded from participation in Medicare, Medicaid and all other federal health care programs. Individuals and entities who have beenreinstated are removed from the LEIE.

LTSS- Long-term services and supports (LTSS) encompass a variety of health, health-related, and social services that assist individuals with functional limitations due to physical, cognitive, or mental conditions or disabilities.

MADP-Medicare Advantage prescription drug (MAPD) plans are a type of Medicare Advantage plan that includes prescription drug coverage.

MassHealth- Massachusetts Medicaid program.

MMP- Medicare-Medicaid Plans participating in CMS' Financial Alignment Demonstration for Medicare-Medicaid enrollees.

Monitoring- Regular reviews performed as part of normal operations toconfirm ongoing compliance and to ensure that corrective actions are undertaken and effective.

NBI MEDIC- National Benefit Integrity Medicare Drug Integrity

Contractor: An organization that CMS has contracted with to perform specific program integrity functions for Parts C and D, and MMPs under the Medicare Integrity Program. The NBI MEDIC's primary role is to identify potential FWA in Medicare Parts C and D.

Non-Compliance- Failure or refusal to act in accordance with the organization's Compliance Program, or other standards or procedures, or with federal or state laws or regulations.

OIG- Office of the Inspector General: The OIG is responsible for audits, evaluations, investigations, and law enforcementefforts relating to DHHS programs and operations, including the Medicare program.

One Care- MassHealth plus Medicare is designed to improve coordination of services provided to dual eligible ages 21-64; the majority of whom have extremely complex medical care needs.

Related Entity- An entity that is related to Commonwealth Care Alliance by

common ownership or control, and either performs some of Commonwealth Care Alliance's management functions (contract or delegation) or furnishes services to Commonwealth Care Alliance members (under an oral orwritten arrangement) or leases real property or sells materials to Commonwealth Care Alliance at a cost of more than $2,500during a contract period.

SCO- Senior Care Options (SCO) is a comprehensive health plan that covers all of the services normally paid for through Medicare and MassHealth. This plan provides services to members through a senior care organization and its network of providers. It combines health services with social support services by coordinating care and specialized geriatric support services, along with respite care for families and caregivers. SCO offers an important advantage for eligible members over traditional fee-for-service care. There are no copays for enrolled members enrolled.

SIU- Special Investigative Unit: the department responsible for investigating allegations of fraud waste, or abuse.

Waste- Overutilization of services, or other practices that, directlyor indirectly, result in

unnecessary costs to any health carebenefit program. Waste is generally not considered to be caused by criminally negligent actions but rather a misuseof resources.

Workforce- Is an employee, non-provider contractor, volunteer, intern, trainee, or consultant who is required to have regular and routine access to a CCA facility, member protected health information, and/or confidential orproprietary information in order to perform their obligations (employment or contractual) and functions for CCA.