Freedom Health, Inc.
Optimum Healthcare, Inc.

Compliance Plan
and
Fraud, Waste, and Abuse (FWA)
Prevention Plan

COMPLIANCE PLAN AND FWA PREVENTION PLAN GOVERNANCE

Freedom Health, Inc. and Optimum HealthCare, Inc., (hereinafter referred to as the "Health Plan") has created this Plan to enforce its commitment to federal and state regulatory obligations.

The Health Plan's Compliance Plan and Fraud, Waste and Abuse (FWA) Prevention Plan (hereinafter referred to as the "Plan") is designed to promote adherence to appropriate standards of business conducted throughout all aspects of the organization's operation and to ensure conformance with applicable federal and state regulatory obligations by the organization and its employees (executive, management, and support staff), partners, vendors, independent agents, independent brokers and its first tier entities, downstream entities, and related entities (FDRs).

The Plan is designed for both Medicare Advantage and Prescription Drug Plan (MA-PD), or Medicare Parts C & D Programs, with direct reference to the compliance elements required in the Medicare Managed Care Manual Chapter 21, and Prescription Drug Benefit Manual Chapter 9 - Compliance Program Guidelines, published by the Centers for Medicare & Medicaid Services (CMS). The plan also complies with all Federal and State requirements, including but not limited to:

- Corporate Integrity Agreement;
- Title XVIII of the Social Security Act;
- Medicare regulations governing parts C and D found in 42 C.F.R. §§ 422 and 423 respectively;
- Patient Protection and Affordable Care Act (Pub. L. No. 111-148, 124 Stat. 119);
- Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191);
- False Claims Acts (31 U.S.C. §§ 3729-3733);
- Federal Criminal False Claims Statutes (18 U.S.C. §§ 287,1001);
- Anti-Kickback Statute (42 U.S.C. § 1320a-7b(b));
- The Beneficiary Inducement Statute (42 U.S.C. § 1320a-7a(a)(5));
- Civil monetary penalties of the Social Security Act (42 U.S.C. § 1395w-27 (g));
- Physician Self-Referral ("Stark") Statute (42 U.S.C. § 1395nn);
- Fraud and Abuse, Privacy and Security Provisions of the Health Insurance Portability and Accountability Act, as modified by HITECH Act;
- Prohibitions against employing or contracting with persons or entities that have been excluded from doing business with the Federal Government (42 U.S.C. §1395w-27(g)(1)(G);
- Fraud Enforcement and Recovery Act of 2009; and
- All sub-regulatory guidance produced by CMS, HHS, and state regulation such as manuals, training materials, HPMS memos, and guides.

Compliance is conforming to activities, practices or policies in accordance with the requirements or expectations of an external authority. In managed care, it means meeting the expectations of those who regulate our business. The best approach to compliance is to take a proactive stance in meeting

our regulatory obligations on a day-to-day basis. An effective Compliance Program must be backed up with solid, ongoing management and organizational processes to prevent, detect, and correct violations of federal and state requirements.

The Health Plan has created this Plan to enforce its commitment to federal and state regulatory obligations and the Corporate Integrity Agreement. The Health Plan maintains high standards of business and personal ethical conduct. The Plan outlines the Organization's Compliance Program, promoting moral and ethical integrity. The Health Plan will take immediate steps to correct any violations of the Plan, including but not limited to imposing appropriate disciplinary actions and implementing corrective measures to prevent future violations. Our Compliance Program is one of the key components of our commitment to the highest standards of corporate conduct.

The integrity and support of the Compliance Plan is made at the highest level, the Organization's Board of Directors. The Compliance Program requires a resolution of the full governing body stating the Health Plan's commitment to compliant, lawful and ethical conduct. Annually, or more frequently as required, the Compliance Officer and Compliance Committee reviews and updates the Plan and presents it for approval to the Organization's Board of Directors. If regulatory or statutory guidance is revised, the Plan will be updated accordingly and presented to the Board for approval.

COMPLIANCE PLAN COMPONENTS

Compliance promotes the prevention, detection, and resolution of instances of conduct that do not conform to Federal and State law and Federal and/or State Health Care Program requirements.

A variety of external methods of compliance enforcement exist including, but not limited to CMS routine monitoring visits, CMS focused monitoring visits, MA-PD self-reporting, industry policing, beneficiary complaints, and Congressional inquiries. The goal of Federal enforcement is threefold: (1) protection of the Medicare beneficiary, (2) protection of the Medicare Trust Fund, and (3) protection of the taxpayer.

As described in the Code of Federal Regulations (CFR) 422.503(b)(4)(vi), the Organization's Compliance Plan, at a minimum, must include the following elements:

1. Written policies, procedures, and standards of conduct that articulate the organization's commitment to comply with all applicable federal and state standards including the compliance obligations in the Corporate Integrity Agreement.
2. The designation of a Compliance Officer and a Compliance Committee who are accountable to senior management.
3. Effective training and education between the Compliance Officer and organization employees.
4. Effective lines of communication between the Compliance Officer and the organization's employees.
5. Enforcement of standards through well-publicized disciplinary guidelines.
6. Procedures for internal monitoring and auditing.

7. Provisions for ensuring prompt response to detected offenses and development of corrective action initiatives.

The Compliance Plan incorporates a comprehensive Fraud, Waste and Abuse Plan to prevent and control fraud, waste and abuse. The Health Plan also addresses its commitment to HIPAA regulations through policies and procedures designed and implemented under the auspices of the Privacy Officer.

POLICIES & PROCEDURES AND STANDARDS OF CONDUCT

The Health Plan has written policies, procedures, and Standards of Conduct that clearly state the organization's commitment to comply with all applicable Federal and State standards, including but not limited to, all applicable statutes, regulations, the Corporate Integrity Agreement and sub-regulatory guidance.

The Health Plan's Standards of Conduct communicate to Associates and FDRs that compliance is everyone's responsibility, from the top to the bottom of the organization. The Standards of Conduct state the overarching principles and values by which the company operates and defines the underlying framework for the Compliance policies and procedures. The Standards of Conduct describe the Organization's expectations that all Associates and FDRs conduct themselves in an ethical manner; that issues of noncompliance, HIPAA, and potential FWA are reported through appropriate mechanisms; and that the reported issue will be addressed and corrected immediately. The Health Plan's Standards of Conduct specify disciplinary actions that can be imposed for violation of laws and ethical standards, noncompliance to the Compliance Program, HIPAA and FWA requirements, including oral or written warnings or reprimands, suspensions, terminations, financial penalties and potential reporting of the conduct to law enforcement. The Standards of Conduct are written in a format that is easy to read and comprehend and is reviewed annually, by the Board of Directors.

Compliance policies and procedures are detailed, specific, and describe the operation of the Compliance Program. The policies and procedures are updated as applicable laws, regulations and other program requirements change and are approved by Senior Management.

The Health Plan has Compliance Policies, Procedures, and Standards of Conduct that:

1. Articulate the Health Plan's commitment to comply with all applicable Federal and State standards.
2. Describe the compliance expectations as embodied in the Standards of Conduct.
3. Implement the operation of the compliance program.
4. Provide guidance to Associates and FDRs on dealing with suspected, detected, or reported compliance, FWA, and HIPAA issues.
5. Identify how to communicate compliance, FWA, and HIPAA issues to appropriate compliance personnel.

6. Describe how suspected, detected or reported compliance, FWA, and HIPAA issues are investigated and resolved by the Health Plan.

7. Includes a policy of non-intimidation and non-retaliation for good faith participation in the compliance program, including, but not limited to, reporting potential issues, investigating issues, conducting self-evaluations, audits, and remedial actions, and reporting to appropriate officials.

8. Includes how the Health Plan conforms to compliance obligations in the Corporate Integrity Agreement.

DISTRIBUTION OF STANDARDS OF CONDUCT AND POLICIES AND PROCEDURES

The Standards of Conduct and policies and procedures are made available to employees and board members at the time of hire (within 90 days of hire), when the standards and policies and procedures are updated, and annually thereafter. The documents are placed on the Intranet (for anytime access) and provided during New Hire and Annual training.

The Health Plans distribute Compliance policies and procedures, Standards of Conduct, and FWA and HIPAA, Corporate Integrity Agreement and Compliance training to all FDRs at the time of contracting (within 90 days), when there are material changes, and annually thereafter. These documents are also made available and distributed through the Compliance-Provider/Vendor Training System, and via email communications directly to the FDRs. FDRs may also utilize their own comparable Standards of Conduct and Compliance policies and procedures, and the plan periodically audits FDRs based on a risk assessment, which includes a review of the FDRs Standard of Conduct and Compliance policies and procedures ensuring they meet the necessary requirements.

COMPLIANCE OFFICER, COMPLIANCE COMMITTEE & HIGH-LEVEL OVERSIGHT

Compliance Officer

The Compliance Officer is responsible for the implementation of the Compliance Program and the Corporate Integrity Agreement. The Compliance Officer defines the program structure, educational requirements, reporting, and complaint mechanisms, response and correction procedures, and compliance expectations of all personnel and FDRs. The Compliance Officer has training and experience working with Medicare programs, with regulatory authorities, and is a member of senior management. The Compliance Officer is a full-time employee and reports directly to the Florida Medicare President. The Compliance Officer is hired with the governing bodies (Board of Directors) approval. The Compliance Officer is independent and does not serve a dual role (Operational and Compliance), only focusing on compliance. The Compliance Officer has direct access and authority to provide unfiltered, in-person reporting to the Florida Medicare President and the Board of Directors. These reports are not routed through any filters and are presented directly to the Florida Medicare President and/or Board of Directors. The Compliance Officer and Compliance Committee reports quarterly to the health plan's governing body (Board of Directors) on the activities and status of the Compliance Program, including issues identified, investigated and resolved by the Compliance Program on a quarterly basis.

The Compliance Officers duties include, but are not limited to, the following:

1. Developing and implementing policies and procedures and practices designed to ensure compliance with State and Federal Regulations, Federal Health Care Program Requirements and the Corporate Integrity Agreement.

2. Reporting to the Compliance Committee and the Board of Directors on at least a quarterly basis. The Compliance Officer provides reports regarding the status of compliance matters to the Florida Medicare President and senior leadership on a more frequent basis. Reports include status of the Compliance Program implementation, identification and resolution of suspected, detected or reported instances of non-compliance/FWA/HIPAA and oversight and monitoring activities.

3. Monitoring of day to day compliance activities by constantly interacting with operational units of the organization. The Compliance Officer also participates in organization wide management meetings.

4. Ensuring adequate educational and training programs are implemented and provide required efficient educational opportunities to officers, governing body, managers, and employees, consultants, volunteers and FDRs. The training is provided at the time of hire and/or contracting, annually, and when material changes occur to ensure that everyone is familiar with the Compliance Program, Standards of Conduct, Compliance Policies and Procedures, and all applicable statutory and regulatory requirements in accordance with the training policy.

5. Developing and implementing methods and programs that encourage reporting of non-compliance, HIPAA, and potential FWA without fear of retaliation or intimidation.

6. Maintaining and managing all reporting mechanisms and closely coordinates with SIU where applicable.

7. Designing and coordinating all investigations (HIPAA, FWA, Compliance), closely working with SIU recommending appropriate or corrective disciplinary actions.

8. Coordinating with other areas to ensure that DHHS, OIG/GSA and CMS Preclusion Lists (as applicable) have been screened with respect to all employees, governing body members, providers and FDRs as required and coordinating any resulting issues with other areas as needed.

9. Maintaining documents for each report of potential noncompliance, HIPAA, FWA received from any source, through the reporting methods (examples are hotline, mail, or in person).

10. Overseeing and reviewing the development and monitoring of corrective action plans.

11. Coordinating all investigation/referrals (internal or external) where applicable (State and Federal regulatory bodies.)

The Compliance Officer has the authority to:

- Interview or delegate the responsibility to interview the Organization's employees and other relevant individuals regarding compliance issues;
- Review company contracts and other documents pertinent to the Medicare Programs;
- Review or delegate the responsibility to review the submission of data to CMS to ensure that it is accurate and in compliance with CMS reporting requirements;
- Independently seek advice from legal counsel;
- Report potential Noncompliance, HIPAA, and FWA to federal and state regulatory agencies and law enforcement;
- Conduct and/or direct audits and investigations of FDRs;
- Conduct and/or direct audits of any area or function involved with federal or state contract requirements; and
- Recommend policy, procedures and process changes.

The Compliance Officer also functions as the organization's Privacy Officer. The regulatory guidelines for designating a Privacy Officer are found at 45 CFR 164.530. The regulatory guidance indicates the roles and responsibilities of the privacy official including the following: training, implementing appropriate administrative, technical and physical safeguards to protect PHI; developing a process for individuals to make complaints; apply appropriate sanctions against members of the workforce; mitigate harmful effects of the use or disclosure of PHI; refraining from intimidating or taking retaliatory action against individuals making complaints; and making provision to change policies and procedures as necessary and appropriate to comply with changes in law.

The Compliance Officer is responsible for carrying out, achieving and maintaining compliance with the Compliance Plan and FWA Prevention Plan. For any Compliance, Fraud, Waste and Abuse, or Privacy issues, the Compliance Officer may be directly contacted. This is the same person to whom whistleblowers may report suspected or actual incidents of non-compliance and fraud, waste and abuse in confidence without fear of retaliation.

Diane Kortsch
Compliance Officer
4200 W. Cypress Street, Suite 800
Tampa, FL 33607
Phone: (813) 506-6107
Fax: (813) 506-6179
Email: Dkortsch@freedomh.com

The Health Plan's Compliance Department provides support to the Compliance Officer in promoting ethical conduct, instilling a company-wide commitment to compliance, and exercising diligence in ensuring the overall Compliance Program requirements are met. For investigation of Compliance Concerns or Fraud, Waste and Abuse issues, the Compliance Officer may delegate the investigation to the Special Investigations Unit (SIU) and/or the appropriate Compliance associate.

Compliance Committee

The Health Plan's Compliance Committee (the "Committee") is a standing subcommittee of the Board of Directors of Freedom Health, Inc. and Optimum Healthcare, Inc., (the "Company") and has oversight responsibility for the Company's compliance with the statutes, regulations and written directives of Medicare, Medicaid, and all other Federal Health Care Programs including the requirements of the Corporate Integrity Agreement.

The principal purpose of the Compliance Committee is to assist the Board of Directors in overseeing the Company's regulatory Compliance Program, policies and procedures, including the Company's: (i) compliance with federal and state laws, rules and regulations applicable to the business of the Company; and (ii) compliance by employees, officers, directors and other agents of, and those providing services for, the Company, with the Company's code of conduct, ethics program, Fraud, Waste and Abuse (FWA) program and related policies.

The Committee shall meet with such frequency and at such intervals as it shall determine is necessary to carry out its duties and responsibilities, the Committee meets quarterly.

The members of the Committee may include executives, staff and/or delegates from business areas within the company, with a variety of backgrounds, who understand the vulnerabilities within their respective areas of expertise, as well as at least two (2) Members of the Board of Directors.

The specific responsibilities and activities of the Compliance Committee are as follows:

1. Developing strategies to promote compliance and the detection of any potential violations of statutes, regulations and written directives of Medicare, Medicaid, and all other Federal Health Care Programs, as well as the Health Plan's Compliance and Ethics Programs, FWA Program and Company Policies and Procedures;

2. In conjunction with the Compliance Officer overseeing the implementation of the Corporate Integrity Agreement;

3. Ensuring that compliance related training, including but not limited to HIPAA, and FWA Training and Education are effective and appropriately completed;

4. Reviewing the Compliance Risk Assessment and the Compliance Monitoring and Auditing work plan;

5. Assisting in reviewing the implementation and monitoring of effective corrective actions;

6. Reviewing effectiveness of the system of internal controls designed to ensure compliance with the statutes, regulations and written directives of Medicare, Medicaid and all other Federal health care programs (as defined in 42U.S.C. s. 1320a-7b(f) in daily operations;

7. Supporting the Compliance Officer's needs for sufficient staff and resources to carry out compliance duties;

8. Ensuring there are appropriate, up-to-date Compliance Policies and Procedures in place;

9. Ensuring that there is a mechanism which enables individuals (i.e., members, employees, and FDRs) to disclose any identified issues or questions associated with the Plan's policies, conduct, practices, or procedures with respect to a Federal Health Care Programs and to report potential instances of noncompliance with respect to Federal Health Care Programs, HIPAA, or instance of FWA confidentially or anonymously (if desired) without fear of retaliation or retribution;

10. Reviewing and addressing reports of monitoring and auditing of areas in which there are risk for program noncompliance, HIPAA or potential FWA and ensures that corrective action plans are implemented and monitored for effectiveness;

11. Providing regular and ad hoc reports on the status of compliance with recommendations to the Board of Directors; and

12. On an annual basis, for so long as the CIA is in effect, reviewing the effectiveness of the Plan's Compliance Program, documenting the Committee's findings and conclusions in writing for submission to the OIG and adopting any related resolutions as required by the CIA.

Governing Body

The Health Plan's governing body is responsible for the review and oversight of matters related to compliance with the Health Plan's Compliance Program, Federal Health Care Program requirements and the Corporate Integrity Agreement. The governing body is also accountable for ensuring effectiveness of the Health Plan's Compliance Program, performance of the Compliance Officer and the Compliance Committee. The governing body meets at least quarterly, includes independent non-executive members and receives Compliance Training and Education as to the structure and operation of the Compliance Program. This enables the governing body to be engaged, to ask questions and to exercise independent judgment over the compliance issues. When compliance issues are presented to the governing body, they make further inquiry and take appropriate action to ensure issues are resolved.

The Governing Body of the Health Plan is tasked with the following duties:

- Determines the adequacy and effectiveness of the Health Plan's Compliance Program;

- Reviews the results of performance and effectiveness assessment of the Compliance Program, Compliance Officer and Compliance Committee;

- Retains compliance expert and/or independent advisor in its oversight of the Compliance Program to perform a review of the effectiveness of the Compliance Program and prepares annual written report;

- Reviews the Compliance Program Review Report;

- Adopts a resolution signed by each member of the board summarizing its review and oversight of the compliance with Federal Healthcare programs and obligations of the Corporate Integrity Agreement;

- Approves the Compliance Plan and Standards of Conduct on an annual basis;

- Understands the Compliance Program structure, through quarterly presentations and annual training;

- Remains informed about Compliance Program outcomes, including results of internal and external audits;

- Remains informed about governmental compliance enforcement activities including but not limited to notice of non-compliance, fines, warning letters, and/or sanctions;

- Receives quarterly updates from the Compliance Officer and Compliance Committee on risk mitigation and compliance efforts;

- Reviews and approves the appointment of the Compliance Officer;

- Receives ongoing updates on the status of organizational risks;

- Receives reports on audits implementation of corrective action plans;

- Receives reports on increase or decrease in number and/or severity of complaints from employees, FDRs, providers, beneficiaries (Source may be from State or Federal agencies);

- Review of dashboards, scorecards, self-assessment tools that reveal compliance issues;

- Evaluates the senior management team's commitment to ethics and the Compliance Program;

- Receives reports on consistent, timely, and appropriate disciplinary actions including issues concerning the Standards of Conduct and allegations of employee misconduct;

- Receives reports on timely response to reported noncompliance, HIPAA, and potential FWA, and effective resolution (ex: Non-recurring issue); and

- Receives reports on internal and external investigations including hotline activity.

TRAINING AND EDUCATION

The Health Plan establishes, implements, and provides effective General Compliance, Fraud, Waste and Abuse (FWA), HIPAA and training and education on the Plan's CIA, Compliance Program and Federal Health Care Program requirements for every officer, director, associate, volunteer, consultant, Board Members (collectively referred to herein as "Associates)" and FDRs (First Tier, Down Stream, and Related Entities) associate. The plan has created a separate policy and procedure for FDR Oversight.

All covered persons receive at least annual training regarding the CIA requirements and plan obligations, Compliance Program, Federal Health Care Program Requirements including the Anti-Kickback Statute and the Stark Law. Covered persons include: (1) all owners who are natural persons and have ownership interest of 5% or more, officers, directors and employees (2) all contractors, subcontractors, agents and other persons who furnish patient care items or services or who perform billing or coding or risk adjustment data functions on behalf of the Health Plan. Covered persons do not include active Medicare providers who are not employees of the Health Plan.

The training and education occurs annually and is part of the Compliance training for new associates.

General Compliance, HIPAA and FWA Training:

- General Compliance, HIPAA, and FWA training including the Anti-Kickback Statute and the Stark Law are provided within 30 days of initial hire and annually thereafter
- Review of the CIA requirements and plan obligations

The training consists of an explanation of the Health Plans' Compliance Program elements, Standards of Conduct, Compliance Policies and Procedures, Fraud, Waste & Abuse and HIPAA definitions, examples, pertinent laws and suspected violation reporting process. It includes:

- An overview of how to ask compliance questions, request Compliance clarification or report suspected or detected noncompliance. Training emphasizes confidentiality, anonymity, and non-retaliation for compliance related questions or reports of suspected or detected noncompliance, HIPAA issues or potential FWA;
- The requirement to report to the sponsor actual or suspected Medicare Program noncompliance, HIPAA issues or potential FWA;
- Examples of reportable non-compliance that an associate might observe;
- A review of the disciplinary guidelines for non-compliance, HIPAA violations or fraudulent behavior. The guidelines will communicate how such behavior can result in mandatory retraining and may result in disciplinary action such as possible termination when such behavior is serious or repeated or when knowledge of a possible violation is not reported;
- Attendance and participation in Compliance, HIPAA and FWA Training Programs as a condition of continued employment and a criterion to be included in associate evaluations;

- A review of policies related to contracting with the government, such as the laws addressing gifts and gratuities for Government employees;
- A review of potential Conflicts of Interest and the sponsor's system for disclosure;
- An overview of HIPAA/HITECH, the CMS Data Use Agreement (if applicable), and the importance of maintaining the confidentiality of Personal Health Information (PHI);
- An overview of the monitoring and auditing process;
- An overview of the CIA and it's requirements;
- A review of the laws that govern associate conduct in the Medicare Program;
- An overview of the Deficit Reduction Act; and
- Laws and regulations related to MA and Part D FWA (i.e., False Claims Act, Anti-Kickback Stark Law, etc.).

Additional specialized or refresher training may be provided on issues posing FWA, compliance, and HIPAA risks based on the individual's job function. Additional training may be provided:

- Upon appointment to a new job function;
- When requirements change;
- When associates are found to be noncompliant;
- As a corrective action to address a noncompliance issue;
- When an associate works in an area implicated in past FWA; and
- Upon a HIPAA violation

General Compliance, HIPAA, and FWA training materials are reviewed and updated whenever there are material changes in regulations, policy or guidance, and at least annually.

Timely completion of the training, quality and timeliness of the content and participation is tracked by Compliance Trainer in a centralized location.

Board Member Training

- Within 120 days of the effective date of the Corporate Integrity Agreement each member of the Board of Directors receives at least two hours of training. The training addresses the corporate governance responsibilities of board members, and the responsibilities of the board members with respect to review and oversight of the Compliance Program;

- New Board Members will receive the specific Board Member Training within 30 days after becoming a member;

- Training includes unique Board Member Responsibilities, risks, areas of oversight areas and strategic methods and approaches to conducting oversight of the Organization.

Measuring Effectiveness
Effectiveness of the training program is made apparent through compliance with all Medicare Program requirements by all associates and FDRs in carrying out their expected job requirements and responsibilities. The Health Plan measures effectiveness in multiple ways, such as:

- Metric Analysis
- Training Quizzes/Tests
- Monitoring of Compliance and FWA Reporting Logs

Training Records

The Health Plan maintains all training records for a period of 10 years. Training records include attendance, topic, attestations and test scores of any tests administered to the Associates.

EFFECTIVE LINES OF COMMUNICATION

The Health Plan has established and implemented effective lines of communication to ensure confidentiality between the Compliance Officer, Director, Employee, Volunteer, Consultant, (collectively referred to herein as "Associates)" and FDRs (First Tier, Down Stream, and Related Entities).

The Health Plan has a system in place to receive, record, respond to and track compliance questions or reports of suspected or detected noncompliance. Such channels of communication are accessible to all and provide a confidential avenue for reporting compliance issues, issues or concerns with the Health Plan's policies, conduct, practices or procedures with respect to the Federal Healthcare Program believed to be a potential violation of criminal, civil or administrative law outside the normal chain of command. All Associates and FDRs are obligated to report compliance concerns and suspected or actual violations through one of the reporting mechanisms as required in the Health Plan's Standards of Conduct and Policies and Procedures.

The Health Plan does not tolerate retaliation or retribution against those who make good-faith reports of potential or suspected violations of the Federal Healthcare Program Requirements. Specifically, the Health Plan maintains a separate policy on non-retaliation and non-intimidation to encourage reporting.

Communicating Compliance Concerns
The Health Plan has established the following mechanisms to allow individuals to report any suspected or confirmed violations or non-compliance of the Federal HealthCare Programs all while remaining anonymous and confidential.

The following methods are made available for reporting suspected or confirmed fraud, waste and abuse, HIPAA, or other compliance concerns as they are identified:

Reporting mechanisms are provided as part of the General Compliance Training, posted on the website included in member and provider materials and posted throughout the Organization.

1. **Internal:**

   - **Secured Website: www.americas1stchoice.ethicspoint.com**
     (24 Hours a Day/7 Days a week)
     - **This website allows easy access 24/7** to report violations of, or raise questions or concerns relating to Compliance, the Health Plan's conduct, practices, procedures or violations of the Federal Healthcare Program.

   - **Compliance Hotline: 1-888-548-0094 (**24 Hours a Day/7 Days a week)
     - The Compliance Hotline is a toll-free resource available twenty-four hours a day, seven days a week to report violations of, or raise questions or concerns relating to, Compliance, the Health Plan's conduct, practices, procedures or violations of the Federal Healthcare Program. Phone calls are directed to Ethics Point via this number. Calls to the Hotline can be made anonymously and confidentially.

   - **Compliance Fax: 1-888-548-0092 (**24 Hours a Day/7 Days a week)
     - Faxes can be sent anonymously and confidentially by Associates, members, and FDRs.

   - **Compliance Email: compliancereporting@americas1stchoice.com**
     (24 Hours a Day/7 Days a week)

   - **Compliance Post Office Box: P.O. Box 152137, Tampa, FL 33684**
     (24 Hours a Day/7 Days a week)
     - Mail can be sent anonymously and confidentially by Associates, members, and FDRs.

Upon receipt of suspected issues of program non-compliance, suspected or potential FWA, or HIPAA, the Compliance Officer or Compliance designee shall record each disclosure within two business days in the disclosure log. The disclosure log shall include a summary, including whether each report received is anonymous or not, the date the investigation was opened, and date closed, and status of the reviews and any corrective action taken.

Compliance reports on a quarterly basis to the Compliance Committee and the Board of Directors on the number of the hotline cases received, what the primary issues or allegations were and whether the allegations were substantiated or not.

To encourage two-way communication, the Compliance Department has developed the below communication strategy:

A. Members

The Health Plan educates their members about identification and reporting of program noncompliance, FWA, and HIPAA concerns.

- Newsletters are sent out quarterly to all members
- All Mechanisms are available on the Corporate Website (under Member links)

B. Associates

1. Compliance Intranet Website

The Compliance Department maintains an intranet website dedicated to educating Associates in key compliance areas related to all lines of business. On the compliance site, associates can find, among other things:

- Policies and Procedures
- Compliance and Fraud Waste and Abuse (FWA) Prevention Plan
- Standards of Conduct and Code of Ethics
- Training (New Hire, Annual Compliance)
- Cubicle Cards, List of reporting mechanisms
- Monthly Compliance Communications

2. Reminders

The Compliance Department provides reminders and helpful tips for Associates to perform their responsibilities in a compliant and ethical manner. Compliance alerts and other Compliance Communications are sent to the entire organization through the Compliance News email distribution and available on the Corporate Intranet.

3. Annual Compliance and Ethics Month

A special time is set annually for the Compliance Department to sponsor special communications and activities to promote awareness of the Health Plan's Compliance Program and dedication to regulatory compliance and business ethics. Various methods of communication are utilized including:

- Posters emphasizing the Health Plan's core values, Compliance Program elements and employee involvement in detecting resolving and preventing issues of non-compliance. These posters remind associates of not just specific rules and regulations, but an overall culture of compliance.

- Articles/communications via corporate e-mail distribution that address important issues and aspects such as ethical/respectful behavior in the workplace, disciplinary actions for non-compliance, the Compliance Monitoring and Auditing Plan and process, FWA, HIPAA reporting process and tips for recognizing FWA or HIPAA issues in the workplace and the importance of our Standards of Conduct and Code of Ethics.

4. Other Company Wide Communication

The Compliance Officer or designee sends periodic Compliance Communication out to all staff members. Communication is focused on the importance of compliance, importance of reporting non-compliance or FWA or HIPAA issues, or related to other important compliance news.

C. FDRs:

The Plan educates FDRs about the identification and reporting of program noncompliance, FWA, and HIPAA concerns through the following:

- Distribution of the Standards of Conduct and Code of Ethics, General Compliance and FWA training and education materials;
- Compliance Policies and Procedures;
- Compliance-Provider/Vendor Training System; and
- Email Communications.

The Plan has an effective way to communicate information from the Compliance Officer to others, such as the Compliance Officer's name, office location and contact information, as well as information about the laws, regulations and guidance. The dissemination of information from the Compliance Officer is made in a timely manner and to all appropriate parties, including FDRs.

There are many external sites provided by regulators where Associates, members, or FDRs can go to report Compliance, FWA and HIPAA issues. Below are a few of the agencies:

- Florida State Attorney General: 1-866-966-7226
- Agency for Health Care Administration, Medicaid Program Integrity at 1-888-419-3456
- Dept. of Financial Services, Div. of Insurance Fraud: 1-800-378-0445
- Office of Inspector General at www.oig.hhs.gov
- Department for Health and Human Services (DHHS): www.hhs.gov/ocr/hipaa
- Centers for Medicare and Medicaid Services: www.cms.gov

ENFORCEMENT OF STANDARDS

All disciplinary standards are enforced in a timely, consistent, and effective manner. Records are maintained for a period of 10 years for all violations and disciplinary actions. Records include the date the violation was reported, a description of the violation, date of the investigation, summary of findings, disciplinary action taken, and the date it was taken. The Organization periodically reviews these records of discipline to ensure that disciplinary actions are appropriate to the seriousness of the violation, fairly and consistently administered and imposed within a reasonable timeframe.

The Health Plan expects all associates and FDRs to report potential violations of Fraud, Waste and Abuse, Medicare Program non-compliance, and HIPAA violations. Failing to report violations or the reporting of violations without "good faith" can lead to disciplinary action up to and including termination.

The Health plan has established reporting mechanisms that all associates and FDRs can utilize to report violations. These mechanisms are reviewed in new hire training, annual training, listed on the intranet, and displayed on employee cubicle cards. All employees must participate in required trainings and assist in the resolution of reported compliance issues.

Following, are the steps of the disciplinary action procedure. The Compliance Officer, or authorized designee, reserves the right to combine or skip steps depending upon facts of each situation and the nature of the compliance violation.

Step 1: Counseling/Training Session
During Step 1, the Compliance Officer, or authorized associate relations designee will notify the associate or FDR of the existing performance/compliance issue. The Compliance Officer, or authorized designee, informs the associate or FDR the nature of the problem or compliance violation outlining expectations and steps the associate or FDR must take to improve performance or resolve the problem. As a result of that discussion, the associate or FDR will have a clear understanding of what is required.

Step 2: Written Warning (Performance Improvement Plan) / Corrective Action Plan
While it is anticipated the performance/compliance issue identified in Step 1 is corrected, this may not always be the case. A written warning involves a more formal documentation of the performance and/or compliance issues and resultant consequences if not corrected.

During Step 2, the Compliance Officer or authorized designee provides a written performance improvement plan or a Corrective Action Plan (CAP) to the associate or FDR.

The performance improvement plan or corrective action plan clearly describes the compliance deficiency and the required improvements or corrections. The Compliance Officer, or authorized designee, communicates with the associate and/or FDR to notify them that the performance or conduct previously discussed continues to be non-compliant and that the counseling/training session has escalated to the second stage. If the associate or FDR completes the corrective action, the disciplinary process may be stopped, and continued monitoring will occur.

Step 3: Extension of Performance Improvement Plan/Corrective Action
If the FDR's or associate's performance and/or adherence to compliance does not improve sufficiently, the Compliance Officer or authorized designee may decide to extend the CAP for a limited period – if the severity of the compliance violation is a low risk.

If the associate's or FDR's behavior does not improve, it may warrant a termination of an associate or the contract. The Company's termination process will be implemented in collaboration with Human Resources and/or Legal. Notification to appropriate State or Federal agencies, when required, will conclude the corrective action plan/disciplinary action.

The Compliance Officer or authorized designee reserves the right to skip Step 1 and Step 2 and skip directly to termination of employee or contract depending on nature of compliance, FWA, and HIPAA violation and the potential harm to enrollees.

Publication of Disciplinary Standards for Associates and FDRs
To encourage good faith participation in the Compliance, FWA, and HIPAA Program, disciplinary standards for associates and FDRs are publicized through various mechanisms.

Associates are notified using the following mechanisms:

- General and Annual Compliance Training;
- Intranet Site; and
- Posters displayed throughout employee work areas.

FDRs are notified using the following mechanisms:

- Distribution of the Standards of Conduct and Code of Ethics, General Compliance and FWA Training and Education materials;
- Compliance Policies and Procedures;
- Compliance- Provider/Vendor Training System; and
- Email Communications.

MONITORING AND AUDITS

The Health Plan performs routine internal compliance monitoring and auditing activities based upon the approved Compliance work plan, inclusive of all lines of business (*Medicare Parts C & D).* Monitoring activities are regular reviews performed of the internal operational areas to confirm ongoing compliance and to ensure that corrective actions are undertaken and effective when issues are detected. Audit activities are formal reviews performed of the internal operational areas to test compliance with a particular set of standards (e.g., policies and procedures, laws and regulations) used as base measures. The Compliance Internal Monitoring and Audit Team test and confirm compliance against Medicare regulations, sub-regulatory guidance, contractual agreements, all applicable federal and state laws, as well as the Plan's policies, protecting against Medicare Program noncompliance, HIPAA and potential FWA.

The following operational area activities are monitored and/or audited by the Compliance Unit, due to high propensity of risk/deficiency (*not an exhaustive list*): Sales and Marketing (inclusive of agent/broker activities), Enrollment/Disenrollment, Credentialing, Claims, Quality Improvement, Provider Relations, Appeals and Grievance, Pharmacy Benefit Formulary Administration (inclusive of but not limited to transition, protected classes, utilization management, and claims processing). The Compliance Unit also performs external audits of FDR functions based upon the results of the FDR Risk Assessment.

The Compliance Officer, Executive Management, and Compliance Committee ensure the internal audit function implemented is appropriate to the organization's size, scope and structure.

When required, participants of the internal monitoring and audit functions may include pharmacists, nurses, physicians, certified public accountants, fraud investigators, SIU staff and other highly skilled staff that have expertise in the areas under review.

The Plan's Compliance Internal Monitoring and Audit Teams report into the Compliance Department and are under the Compliance Officer leadership. The Monitoring and Audit Teams test and confirm such compliance against Medicare regulations, sub-regulatory guidance, contractual agreements, all applicable federal and state laws, as well as the Health Plan's policies, protecting against Medicare Program noncompliance, HIPAA and potential FWA. The monitoring and audit results are reported to the Florida Medicare President, Compliance Committee, and the Board of Directors at least quarterly.

The Organization has developed a strategy to monitor and audit its FDRs, to ensure they are in compliance with applicable laws and regulations. The contractual arrangements with First Tier Entities provide for routine and random auditing.

Risk Assessments

An effective monitoring and auditing program begins with a comprehensive Internal Risk Assessment. In order to establish an effective system for monitoring and auditing, the Health Plan utilizes a risk assessment tool that takes into account operational areas. The operational areas are assessed for potential and inherent compliance issues (including noncompliance, FWA, HIPAA). Identified issues are categorized and prioritized by risk types and levels of risk they present to beneficiaries and the Organization's operational and compliance program. An FDR risk assessment is done independent of the operational area risk assessment.

The Operational Monitoring Work Plan

- Compliance selects key metrics in each area. Monitoring activities are selected based on the risk assessment which is continually updated and maintained throughout the year as well as other key regulatory metrics. Each operational area is expected to monitor these activities and report them to Compliance.
- All of these activities are listed on the monitoring work plan. The work plan consists of a listing of the department(s) monitored, date monitoring efforts began, type of monitoring conducted (report analysis and/or sample reviews), description of metric/activity monitored; finding and outcomes of monitoring efforts and description of any corrective/remediation action taken as a result of the findings.
- The results of monitoring activities are presented to Executive Management, the Compliance Committee, and the Board of Directors.

The Audit Work Plan

- Based on the risk assessment, executive feedback, and results from the monitoring work plan, activities are selected and independently validated through audits by compliance;
- These activities are listed on the Audit Work Plan and organized by quarter;
- The Audit Work Plan includes the activity audited; audit type; area/department audited; audit schedules (including start and end dates); audit status (scheduled, open or closed),

type of auditor (internal staff vs external firm); audit objectives; and findings/outcomes, as well as a description of any corrective/remediation action taken as a result of the finding;

- The final audit report is reviewed and approved by the Compliance Officer and/or designated staff;
- The results of the audit activities are presented to Executive Management, the Compliance Committee, and the Board of Directors.

Tracking and Documenting Compliance efforts

The Plan tracks and documents all internal monitoring and auditing activity and compliance efforts. The Monitoring and Audit Teams utilize a variety of means to track and document such efforts via the following internally created tools: audit tracker, corrective action and issues tracker, work templates/tools, dashboards, and other reports and mechanisms.

Regularly, the Monitoring and Audit Teams' overall activity results/reports are discussed with the Compliance Officer, to apprise or discuss activity status/results and any issues of noncompliance identified. The Compliance Officer communicates these summarized results to the Florida Medicare President, the Compliance Committee, and the Board of Directors.

The Board of Directors retains an individual with expertise in compliance with Federal Health Care Program Requirements to perform a review of the effectiveness of the Health Plan's Compliance Program and prepare a written report. The Board of Directors reviews the reports as part of its review and oversight of the Compliance Program. A copy of the report is provided to the OIG annually.

OIG/GSA Exclusions

The Organization reviews the HHS Office of the Inspector General (OIG) List of Excluded Individuals and Entities (LEIE) and the US General Services Administration (GSA) System for Award Management (SAM) Exclusion Database prior to the hiring or contracting of any employee (new hires, temporary, volunteer, consultant), governing body member, or FDR, and monthly thereafter, to ensure that none of these entities are excluded or become excluded from participation in federal programs. Monthly screening is essential to prevent inappropriate payment to providers, pharmacies, and other entities that have been added to the exclusions lists. The Health Plan does not submit administrative costs in connection with excluded non-health care contractors. The Organization performs audits on a sample of FDRs annually to validate adherence to this requirement. The Human Resources Department conducts these reviews for all employees, including new employees, temporary employees, volunteers, consultants and governing body members.

Auditing by Federal Agencies or External Parties

CMS has the discretionary authority to perform audits to evaluate or inspect any books, contracts, medical records, patient care documentation, and other records of the Health Plans, and FDRs that pertain to any aspect of services performed, reconciliation of benefit liabilities, and determination of amounts payable under the contract or as the Secretary may deem necessary to enforce the contract.

The Health Plan allows access to any auditor acting on behalf of any regulatory agency to conduct an on-site audit. On-site audits require a thorough review of required documentation. Such reviews include any information needed to determine compliance with contracts and regulations.

The Health Plan and FDRs provide records to regulatory bodies or its designee, immediately upon request. The Health Plan and FDRs are required to fully cooperate with all regulatory and sub regulatory agencies. The Health Plans will provide CMS and/or CMS designated contractors with access to all requested facilities and records associated in any manner with the Medicare Parts C or D Program.

ENSURING PROMPT RESPONSE & DEVELOPMENT OF CORRECTIVE ACTIONS

The Health Plan has established and implemented procedures and a system for promptly responding to compliance/FWA/HIPAA issues as they are raised, investigating potential violations as identified in the course of self-evaluations, reporting, audit and monitoring activities, correcting such problems promptly and thoroughly to reduce the potential for recurrence, and ensuring ongoing compliance with State and Federal requirements, Federal Health Care Programs and the Corporate Integrity Agreement.

When the Organization discovers evidence of potential misconduct (example: related to payment or delivery of items or services under contract) it conducts timely, reasonable inquiry into that conduct.

1. The Plan implements appropriate corrective actions, (i.e. repayment of overpayments, disciplinary actions against responsible individuals in response to any confirmed violations.
2. The Organization also has procedures to voluntarily self-report potential compliance, HIPAA, or fraud violation to appropriate state and federal regulatory agencies.

Conducting a Timely Reasonable Inquiry of Detected Offenses

The Health Plan's Compliance Team conducts a timely and well-documented reasonable inquiry into any potential noncompliance, HIPAA, or FWA violation. The potential violation may be discovered through a hotline, a website, an enrollee complaint, during routine monitoring or self-evaluation, an audit, or by regulatory authorities. Regardless of how the potential violation is identified, a reasonable inquiry is initiated as quickly as possible but no later than two weeks after the date the potential incident was identified.

1. An inquiry is officially initiated and recorded within 2 business days upon receipt of the inquiry. Details are recorded in the disclosure log including dates, source of investigation, issue type, corrective action, and closure date.
2. The Compliance Officer or Compliance designee shall make a preliminary good faith inquiry into the allegations to ensure all necessary information is obtained to determine whether further review should be conducted. For any disclosure that (1) permits a determination of the appropriateness of the alleged improper practice; (2) provides an opportunity for taking corrective action, the Plan shall conduct an internal review of the allegations, ensure proper protocols are followed and responses are provided in a timely manner. The Plan also provides the complainant with information regarding expectations of a timely response, confidentiality, non-retaliation, and progress reports (to the extent allowed by the investigation).

3. The investigational research efforts include, but are not limited to:
    a. Collection of the facts;
    b. Review of regulatory guidance;
    c. If required, contact with members, and/or providers;
    d. Data analysis of the issue; and
    e. If required, meeting with area leaders and senior management.
4. Confidentiality is maintained by minimizing the number of people privy to investigational information. Information is only shared with applicable parties.
5. If warranted, a corrective action plan is issued.
6. Upon completion of corrective action and review for validation, state and/or federal agencies may be notified depending on severity of the issue. If warranted, members, providers, and or other parties are notified of the issue. Once all appropriate parties are notified the case is closed.

Corrective Actions

The Organization corrects Compliance, HIPAA, and FWA violations promptly after they are identified. In the case of violations which have been clearly demonstrated to be founded and supported by evidence, a Corrective Action Plan (CAP) is issued. The CAP is designed to correct the underlying problem that resulted in program violations and to prevent future noncompliance. The CAP also has timeframes for specific achievements towards addressing the deficiency. For FDRs, detailed ramifications are also listed in the written agreement if the FDR fails to implement the corrective action satisfactorily.

A follow up is done on all CAPs to ensure that the misconduct has been properly addressed and continued monitoring is put into place. If corrective actions are not properly implemented or corrected, additional disciplinary measures are taken including and up to termination of the associate or contract. Documentation is maintained on all deficiencies identified and corrective actions taken.

Self-Reporting Potential Fraud, HIPAA, or Noncompliance

The Organization has developed a process to voluntarily self-report FWA, HIPAA and program noncompliance as it believes it's an important component of maintaining an effective compliance program.

The Compliance Officer or a designated appointee investigates potential HIPAA, fraudulent or noncompliant activities to make a determination whether a violation has occurred. For Medicare, when the Organization does not have time, resources, or experiences to adequately investigate potential fraudulent misconduct, the matter is referred to the MEDIC within two weeks from the potentially fraudulent activity discovery.

The Organization concludes all investigations of potential misconduct within a reasonable time period after the potential violation is discovered. If after conducting a reasonable investigation, the organization determines a violation has occurred, the conduct is promptly referred to the appropriate regulatory agency or government authorities such as OIG or CMS.

FRAUD, WASTE AND ABUSE (FWA) PREVENTION PLAN

The FWA Prevention Plan is a subset of the overall Compliance Program at the Health Plan's. Elements of the FWA prevention activities are integrated into each of the seven elements of an effective compliance program. Please refer to each of the sections outlined below for details on how the Health Plan prevents fraud, waste and abuse:

- Written Policies and Procedures and Standards of Conduct and Code of Ethics;
- Compliance Officer and Compliance Committee;
- Training and Education;
- Effective Lines of Communication;
- Enforcement of Standards through well publicized disciplinary guidelines;
- Monitoring and Auditing;
- Prompt Responses to Detect Offenses and Corrective Action Procedures.

Fraud Waste and Abuse definitions, examples, important laws, and the SIU area are highlighted below.

What is Fraud, Waste, and Abuse?

Fraud: An intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to oneself or some other person. It includes any act that constitutes fraud under applicable Federal or State law.

Waste: An overutilization of services or improper billing practices that result in unnecessary costs. Generally, not considered caused by criminally negligent actions but rather through the misuse of resources.

Abuse: Gross negligence or reckless disregard for the truth in a manner that could result in an unauthorized benefit and unnecessary costs either directly or indirectly.

Definitions and examples of fraudulent activities are cited below.

Health Plan Fraud

Fraud committed by the Health Plan is defined as acts committed through deception, misrepresentation or concealment by the health plan's employees as directed by leadership of the health plan. Such acts can include but are not limited to:

- Failure to provide medically necessary services
- Marketing schemes
- Improper bid submissions
- Payments for excluded drugs
- Multiple billing

- Inappropriate formulary decisions
- Inappropriate enrollment/disenrollment
- False information
- Inaccurate data submission

Fraud by Agents/Brokers
Fraud committed by agents/brokers is defined as deception, misrepresentation or concealment by a licensed representative to obtain something of value for which he/she would not otherwise be entitled. Some examples of agent/broker fraud can include but are not limited to:

- Helping individuals fill out their enrollment information so they will be eligible for insurance
- Enrolling a group of individuals to form a nonexistent company
- Falsifying location of a group to gain insurance or obtain lower premium rates
- Adding false individuals to the group to avoid being medically underwritten
- False advertising

Fraud Due to Misrepresentation of Enrollment Information
Fraud due to misrepresentation of enrollment information is defined as commission of an act of deception, misrepresentation or concealment, or allowing it to be done by someone else, to obtain coverage for which one would not otherwise be entitled. Examples of eligibility fraud can include but are not limited to:

- Members not meeting the eligibility requirements (e.g., not working the required number of hours, not receiving a wage)
- Not disclosing medical conditions on an application

Claims Fraud
Examples for Claims Fraud can include but are not limited to:

- Provider is not in the insured's geographic region
- Member is in a different state than the company and no group affiliations exist for that state
- Large bills incurred just prior to term date or immediately after effective date
- Inconsistencies in company information versus medical records

Provider Fraud
Provider fraud is defined as "the devising of any scheme by any provider of health care or services to defraud for the purpose of personal or financial gain by means of false or fraudulent pretenses, representations, or promises." Examples of provider fraud can include but are not limited to:

- Billing for services not rendered
- Providing "free" services and billing the insurance company
- Nonqualified practitioners billing as qualified practitioners

- Providers being rewarded for writing prescriptions for drugs or products
- Billing for non-covered services using an incorrect code by the American Medical Association (AMA) Current Procedural Terminology (CPT®), Healthcare Common Procedural Coding System (HCPCS) and/or diagnosis codes to have the services covered

Pharmacy Fraud
Examples of pharmacy fraud can include but are not limited to:

- Filling less than the prescribed quantity of a drug
- Billing for brand when generic drugs are dispensed
- Billing multiple payors for the same prescriptions
- Dispensing expired or adulterated prescription drugs
- Forging or altering prescriptions
- Refilling prescriptions in error

Examples of pharmacy benefit management fraud can include but are not limited to:

- Prescription drug switching
- Unlawful remuneration
- Prescription drug shorting
- Failure to offer negotiated prices

Member Fraud
Member fraud is defined as the commission of acts of deception, misrepresentation or concealment by any policyholder or group of policyholders in order to obtain something of value to which they would not otherwise be entitled. Examples of member fraud can include but are not limited to:

- Alteration of bills
- Submission of false claims
- Applying for insurance when you know you are not eligible
- Reselling drugs on the black market
- Doctor shopping
- Identity theft
- Forging or altering prescriptions
- Prescription stockpiling
- Improper coordination of benefits
- Failure to disclose information on applications, accident inquiries, continuation of benefits (COB) and full-time student information requests

Important Federal Laws:
There are several laws that address health care fraud. These laws define fraud and establish the framework for the prosecution of criminal acts and the initiation of civil suits by injured parties. Listed below are a few of the laws that address health care fraud:

Federal False Claims Act (FCA) – 31 U.S.C. Title 3729
The False Claims Act addresses any person or entity that does any of the following:

- Knowingly presents, or causes to be presented, to an employee of the United States government a false or fraudulent claim for payment or approval
- Knowingly makes, uses or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the government
- Conspires to defraud the government by getting a false or fraudulent claim allowed or paid
- Knowingly makes, uses or causes to be made or used, a false record or statement to conceal, avoid or decrease an obligation to pay or transmit money to the government
- Has actual knowledge of the information
- Acts in deliberate ignorance of the truth or falsity of the information
- Acts in reckless disregard of the truth or falsity of the information; no proof of specific intent to defraud is required

The False Claims Act imposes two sorts of liability:

- The submitter of the false claim or statement is liable for a civil penalty, regardless of whether the submission of a claim causes the government any damages and even if the claim is rejected.
- The submitter of the claim is liable for damages that the government sustains because of the submission of the false claim.

Under the False Claims Act, those who knowingly submit or cause another person to submit false claims for payment by the government, are liable for three times the government's damages plus civil penalties of $11,665 to $23,331 per false claim.

Whistleblower (Qui Tam) Protection – 31 United States Code Service (USC) 3730 (h)
The whistleblower provision protects employees who assist the federal government in investigation and prosecution of violations of the False Claims Act. Whistleblower protections apply only to actions taken in furtherance of a viable False Claims Act case, which has been, or is about to be, filed. The provision prevents retaliation against employees such as firing them for assisting in the investigation and prosecution. If any retaliation does occur, the employee has a right to obtain legal counsel to defend the actions taken.

Physician Self-Referral Prohibition Statute commonly referred to as the "Stark Law" 1877 of the Social Security Act (42 USC 1395nn)
This statute prohibits physicians from referring Medicare patients for certain designated health services (DHS) to an entity with which the physician or a member of the physician's immediate family has a financial relationship, unless an exception applies. It also prohibits an entity from

presenting or causing to be presented a bill or claim to anyone for a DHS furnished as a result of a prohibited referral.

Anti-Kickback Statute Section 1128(b) of the Social Security Act (42 USC 1320a-7b (b))
The federal anti-kickback laws prohibit health care professionals, entities and vendors from knowingly offering, paying, soliciting or receiving remuneration of any kind to induce the referral of business under a federal program. In addition, most states have laws that prohibit kickbacks and rebates. Remuneration under the federal anti-kickback statute includes the transfer of anything of value, directly or indirectly, overtly or covertly, in cash or in kind. Violators are subject to criminal sanctions such as imprisonment, as well as high fines, exclusion from Medicare and Medicaid, very costly civil penalties and possible prosecution under many similar state laws. The anti-kickback law is extremely broad and covers a wider range of activities than just traditional kickbacks. Federal regulations include safe harbors that protect certain technically prohibited activities from prosecution.

Antitrust Laws
State and federal antitrust laws prohibit monopolistic conduct and agreements that restrain trade. The health plan is committed to competition and consumer choice in the marketplace. All health care professionals, entities and vendors must adhere to the antitrust laws and must avoid any agreements or understandings with competitors on price, customers, markets or other terms of dealing and avoid trade practices that unfairly or unreasonably restrain competition in dealings with providers or customers.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
HIPAA was enacted to improve the efficiency and effectiveness of health information systems by establishing standards and requirements for the electronic transmission of certain health information. Regulations established standards for certain electronic transactions, along with minimum privacy and security requirements for individually identifiable health information that is held by covered entities. The protection of individual information may decrease chances of misuse of the information involving fraudulent activities. In addition, these measures may decrease the risk of identity theft.

Special Investigations Unit (SIU)
The health plan has established a Special Investigations Unit (SIU) to identify, investigate and resolve instances of fraud, waste and abuse committed by internal and external sources. These sources include providers, facilities, vendors, FDRs, employees, consulting partners, and members. The Health Plan's SIU resides within the Compliance Department and works in collaboration with the Compliance Officer to defend against criminal behavior, unethical conduct, instances of false claims and improper billing and coding practices, and other schemes that adversely impact the safety of our members and the quality of health care services delivered.

SIU is responsible for the following:

- Reducing or eliminating Parts C and D benefit costs due to FWA;
- Ensuring proper value of Parts C and D benefits, including correct pricing, quantity, and quality;

- Utilizing real-time systems that ensure accurate eligibility, benefits, services, refills, and pricing and that identify potential adverse drug interactions and quality of care issues;
- Reducing or eliminating fraudulent or abusive claims paid for with federal dollars;
- Preventing illegal activities;
- Identifying members with drug addiction problems and other overutilization issues;
- Identifying and recommending providers for exclusion, including those who have defrauded or abused the system;
- Referring potential cases of illegal drug activity, including drug diversion, to the MEDIC, and/or law enforcement and conducting case development and support activities for the MEDIC, and law enforcement investigations;
- Assist law enforcement by providing information needed to develop successful prosecutions; and
- Provide fraud awareness training to the employees of the Sponsor.

The Compliance area and the SIU work with multiple departments to ensure all employees have been trained on identifying and reporting FWA cases as well as ensuring control mechanisms are in place to prevent Fraud, Waste and Abuse.

Below are a few examples of control points in some of the departments:

Pharmacy Benefit Manager (PBM)
The SIU area works with the PBM to provide ongoing oversight of the Part D FWA prevention program.

The PBM utilizes a vendor to review claim activity and to conduct onsite pharmacy audits. The vendor is very well known in the industry and is versed in conducting pharmacy audits.

They utilize software, which is a combination of relational database technology, predictive modeling and highly developed algorithms to review claims and is designed to:

- Audit claims
- Deter, identify and refer fraudulent claims submission
- Identify recoveries
- Protect the financial integrity of the prescription benefit
- Identify areas of concern and potential problems

Prescriptions that require further inspection are identified for either a desktop or onsite audits, audit activity reports are provided for each customer.

The contracted vendor selects pharmacies for onsite audits and inspects prescriptions monthly as a part of the comprehensive site review process.

Desk Top Audits
The audit department at the PBM conducts a complete analysis of pharmacy provider prescription claims. It utilizes 100% of the claims that process through the central claims system.

Data is analyzed and reviewed using approximately 90 edits to find patterns, anomalies, errors, and potentially fraudulent activity that are designed to detect medication waste.

Onsite Audits
The onsite audit program is a general overview and examination of the pharmacy's practices, procedures and general facility. Performed by pharmacy professionals, onsite audits are designed to enhance program compliance and provide a sentinel effect to deter fraudulent or deviant behavior.

The onsite audit is also used to capture credentialing information. Onsite auditors will note items such as counseling availability, hours of operation, languages spoken by the staff and other special services provided, wholesalers used, and other quality-related items.

The onsite audit program provides overpayment and fraud activity review. The program utilizes a suite of edits to automatically select, rank and score pharmacies across over 50 distinct criteria. The use of predictive modeling techniques as well as a proprietary 'fraud formulary' help identify not only individual stores for review, but specific prescriptions that may be worthy of actual inspection.

Selection
The PBM generates various summary reports to statistically identify pharmacies deviating from the normal plan percentages. Through these specialized reports, which are incorporated into a proprietary ranking report card, the PBM selects a number of pharmacies to conduct onsite reviews. This selection process increases the odds of detecting fraudulent activity. Additional pharmacies may be selected as a result of State or client referral, patient complaints, physician complaints and or peer complaints.

Preparation & Visit
Prior to visiting a pharmacy for an onsite audit, the PBM or its designee schedules appointments with the pharmacy's manager/owner, and in some instances, make arrangements through the corporate offices of chains in order to have a regional or district manager or other assistant available at the time of the audit. In preparing for the review, targeted prescriptions and patient records are selected prior to arrival for audit at the pharmacy. During all onsite visits, auditors collect information on store hours, patient counseling, clinical references, and other 'credentialing-type' information. The claims that are selected for audit are scanned into a laptop based program and stored securely.

Fraud, Waste & Abuse Criteria and Variables
Multiple variables and criteria are used to identify claims to be audited:

- high dollar claims
- unusual/high quantities
- unusual day's supply
- excessive claims for controlled substances
- brand use percent

- controlled substance dispensing or prescribing percent
- excessive rejections
- high dollar or prescription volume for pharmacies or physicians
- unusual package size items
- less frequently billed items
- items requiring special and/or restricted protocols
- duplicate (double) billings
- early refills
- refills outside of State or Federal allowances (high number of refills)
- excessive refills
- incorrect quantity for days' supply
- insulin and supply billing
- high DAW percent
- use of terminated NDC's
- billing incorrect package sizes
- physicians billing outside specialty
- failure of physician ID validation for CII Drugs
- high member Utilization
- high compound percent
- high $ compound claims
- appearance of split billing to increase fees or bypass early refill edits
- high percent of PA overrides
- billing during periods when the pharmacy is closed, after hours or holidays
- excessive reversal rates
- high cost injectable
- refill patterns
- DUR interactions
- invalid or terminated DEA, license numbers
- infusion medications per member

Additional variables are reviewed when examining hard copy prescriptions-

- completeness of prescription
- member and physician information
- medication descriptions
- directions for use
- refill directions
- DAW information
- notes (PA, additional refill information etc.)

Sales/Marketing

The Compliance area works closely with our Sales/Marketing area to prevent FWA.

- All agents are trained by the Health Plan's Compliance Department or by using the Compliance Department approved training material

- Only CMS approved marketing materials are used
- Audit of Agents' files to verify licensure and OIG/DFS blacklist
- Random check of actual marketing material
- "Ride Along" on sales calls
- Surprise/secret visits to seminar presentations
- Rapid disenrollment rate and cancellation rate analysis
- Member complaints on agents received from member services call logs, CMS complaint tracking module, grievance department logs and state agency referred cases

Claims
The Health Plan has proactively added in edits into our claims system to ensure FWA is prevented and detected.

Below are the edits inputted into the system:

- Invalid diagnosis codes
- Invalid procedure codes
- CPT/Place of service miss-match
- Invalid CPT/modifier combination
- Excessive/Invalid units
- Incorrect bill types
- Duplicate services
- 3 day/1-day payment window

Health Services
The Health Services department may identify scenarios during authorization and utilization reviews that indicate potential FWA

- Prior authorization process – some of the services susceptible to fraud, waste and abuse may be identified through the prior authorization process. The process requires review of medical record documentation to support the need for the requested services. During this process, other authorizations are reviewed for consistency and could determine a pattern of fraudulent activity on occasion.
- Utilization management – this process involves the review of provider utilization of resources, especially in the area of over utilization identifying outliers of plan wide metrics.

Health Services refers any cases where FWA may be identified to SIU.

Enrollment
The Enrollment department refers suspicious enrollments to the SIU for investigation.