☒ **Freedom Health, Inc.** ☒ **Optimum HealthCare**	**Policy Title: Written Policies, Procedures and Standards of Conduct** **Primary Department: Compliance** **Policy Number: COMP 01** ☒ **Medicare**
Approved By: Diane E.A. Kortsch 04.30.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 3/28/2012** | **Effective Date: 4/1/2012** **Revision Date(s): 09/01/2012; 04/01/2016; 07/17/2017, 11/09/2018, 04/30/2020** **Incorporated previous COMP14, COMP18 & COMP26**
Reference: 42 C.F.R. § 400, 403, 411, 417, 422, 423, 1001, and 1003; 45 CFR 160, 162, 164; Medicare Managed Manual Chapter 21; Prescription Drug Benefit Manual Chapter 9; Title I of the Social Security Act; 42 CFR 422.503(b)(4)(vi), 42 CFR 423.504(b)(4)(vi); The Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG").	

POLICY:

The Plan is committed to adhering to all applicable Federal and State regulations as well as the Corporate Integrity Agreement. The Plan, via its Compliance Department, develops policies and procedures to promote and ensure that every officer, director, employee, consultant, and volunteer (collectively referred to herein as "Associates)" and FDRs (First Tier, Down Stream, and Related Entities) are in compliance with all applicable laws, rules, and regulations.

The Plan has compliance policies, procedures, and Standards of Conduct that:

1. Articulate the Plan's commitment to comply with all applicable Federal and State standards including the Corporate Integrity Agreement;
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 Plan; and
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.

PROCEDURE:

A. Laws & Regulations:

The following Laws and regulations were considered in Standards of Conduct, policy and procedures, and training.

- Corporate Integrity Agreement
- Title XVIII of the Social Security Act;
- Medicare regulations governing parts C and D found at 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 AHCA, CMS and HHS such as manuals, training materials, HPMS memos, and guides

B. Standards of Conduct

The Plan's Standards of Conduct are written in a format that is easy to read and comprehend. The Plan's Standards of Conduct communicates 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 Plan'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 the reported issue will be addressed and corrected immediately.

The 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 Standard of Conduct is approved and supported by the Plan's entire governing body on an annual basis. The Standards of Conduct is updated as required to incorporate changes in applicable laws, regulations and other program requirements.

The Plan's Standards of Conduct covers at a minimum:

- Corporate Integrity Agreement
- The Code of Ethics
- The Health Plan's mission and core values
- Compliance Program
- Fraud, Waste, and Abuse
- HIPAA
- Importance of Reporting Violations
- Non-Intimidation, Non-Retaliation
- Disciplinary Actions
- Business/Company Conduct

C. Policies and Procedures

Compliance Policies and Procedures are detailed, specific, and describe the operation of the Compliance Program. The Compliance Policies and Procedures include the following topics:

- Compliance Policies and Procedures and Standards of Conduct
- Responsibility of Compliance Officer, Compliance Committee, Board of Directors
- Compliance, HIPAA, and FWA Training Requirements
- Audits, Monitoring, and Corrective Action Plans
- OIG/GSA Exclusion Verifications
- Effective Lines of Communication
- How potential or actual violations are reported (mechanisms)
- How suspected, detected or reported Compliance, HIPAA, and FWA issues are investigated, addressed, and remediated
- Non-Intimidation & Non-Retaliation
- Conflict of Interest
- FDR Oversight

- HIPAA Privacy and Breach Notification
- Disciplinary Standards
- Record Retention
- Anti-Discrimination
- Disaster and Emergency Declaration
- Sales and Marketing/CTM Oversight
- FWA
- Agent Oversight
- Marketing Member Materials
- Delegation Oversight

The policies and procedures are assessed at least annually and updated as applicable laws, regulations, and other program requirements change.

Annually, business area leaders enterprise wide are required to attest to the accurateness, completeness and content of their departmental policies and procedures. This process ensures that policies are maintained with the most current regulations and requirements.

All Compliance Policies and Procedures are available to all associates and FDRs and compliance with the Plan's policies and procedures is an element used in evaluating the performance of all associates.

D. Distribution of Compliance Policies and Procedures and Standards of Conduct

- **Associates**

  The Plan distributes compliance policies and procedures and Standards of Conduct to all Associates:

  - Within 90 days of hire
  - Whenever policies and procedures/Standards of Conduct are revised or updated; and
  - Annually thereafter

  The documents are provided during new hire orientation via the online portal, placed on the Intranet (for anytime access), and reviewed during annual training.

- **FDRs**

  The Health Plan distributes Compliance Policies and Procedures and Standards of Conduct to FDRs at the time of contracting (within 90 days), when there are material changes, and annually thereafter. These documents are made available and distributed through the Compliance-Provider/Vendor Training System and/or via e-mail

communication to the FDR. FDRs may also utilize their own comparable policies and procedures, and Standards of Conduct. The plan periodically audits FDRs based on a risk assessment, which includes a review of the FDRs Compliance Policies and Procedures, and Standards of Conduct.

☒ **Freedom Health, Inc.** ☒ **Optimum HealthCare**	**Policy Title: Compliance Officer, Compliance Committee & High-Level Oversight** **Primary Department: Compliance** **Policy Number: COMP 02** ☒ **Medicare**
Approved By: Diane E.A. Kortsch 05/08/2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 03/28/2012** | **Effective Date: 04/01/2012** **Revision Date(s): 03/30/2016; 07/28/2017, 08/21/18, 12/07/2018, 06/11/2019, 05/08/2020** **09/01/2012: Incorporated COMP18 & COMP28**
Reference: Prescription Drug Benefit Manual Chapter 9; Medicare Managed Manual Chapter 21; Health Insurance Portability and Accountability Act; and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG")	

POLICY:

The Health Plan has a designated Compliance Officer and Compliance Committee who report directly to and are accountable to the organization's President of Medicare Markets. The Health Plan's governing body (Board of Directors) exercise reasonable oversight with respect to implementation and effectiveness of the Compliance Program.

1. The Compliance Officer, vested with the day-to-day operations of the Compliance Program, is an employee of the MAO or Part D Sponsor, or of its parent organization or corporate affiliate.
2. The Compliance Officer and the Compliance Committee report quarterly to the Health Plan's governing body (Board of Directors) on compliance activities and the status of the Compliance Program.
3. The governing body (Board of Directors) is knowledgeable about the content and operation of the Compliance Program and exercises reasonable oversight with respect to implementation and effectiveness of the Compliance Program.

PROCEDURE:

A. Compliance Officer

The Compliance Officer is responsible for the implementation and maintenance of the Compliance Program. 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 and Medicaid programs, with regulatory authorities, is a

fulltime employee, member of the Senior Management Team, is not a subordinate to Legal Counsel or the Chief Financial Officer, and reports directly to the President of Medicare Markets. The Compliance Officer does not act in any capacity as legal counsel or supervising any legal counsel functions for the organization. The Compliance Officer is put into place with the Health Plan's governing body (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 Health Plan's President of Medicare Markets and the Board of Directors. These reports are not routed through any filters and are presented directly to the President of Medicare Markets and/or Board of Directors.

The Health Plan will report to the OIG in writing within five days should there be any changes in the identity of the Compliance Officer or in their ability to perform the duties necessary to meet the obligations in the Corporate Integrity Agreement.

The duties of the Compliance Officer include:

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 President of Medicare Markets 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 bodies, managers, employees, consultants, volunteers and FDRs. The training is provided at the time of hire, 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) and closely working with SIU. Implementing appropriate or corrective disciplinary actions.

8. Coordinating with other areas to ensure that DHHS OIG and GSA exclusions lists have been checked with respect to all employees, governing body members, and FDRs monthly 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 on 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 Health Plan's employees and other relevant individuals regarding compliance issues;
- Review of Health Plan's contracts and other documents pertinent to the Medicare Program;
- 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 non-compliance, HIPAA, and FWA to Federal and State Regulatory Agencies and/or 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 Health Care Programs;
- Recommend policy, procedures and process changes.

B. Compliance Committee

The Compliance Committee (also referred to herein as "Committee") has oversight responsibility for the Health Plan's compliance with the statutes, regulations and written directives of Medicare 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 Health Plan's regulatory Compliance Program, policies and procedures,

including the Health Plan's: (i) compliance with federal and state laws, rules and regulations applicable to the business of the Health Plan's; and (ii) compliance by employees, officers, directors and other agents of, and those providing services for, the Health Plan's, with the Health Plan'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, but in any case the committee meets at least quarterly.

The members of the Committee include executives, staff and/or operational area delegates from business areas within the Health Plan with a variety of backgrounds, those 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 and all other Federal Health Care Programs, as well as the Health Plan's Compliance and Ethics Programs, FWA Program and the Health Plan's 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 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 Health Plan's policies, conduct, practices, or procedures with respect to Federal Health Care Programs and to report potential instances of non-compliance 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 non-compliance, HIPAA or potential FWA and ensures that corrective action plans are implemented and monitored for effectiveness; and

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

12. On an annual basis, for so long as the CIA is effective, reviewing the effectiveness of the Health 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.

C. Governing Body (Board of Directors)

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 Health Care 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 notices 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

D. Management involvement in Compliance Program

The Health Plan's Compliance Officer reports directly to the President of Medicare Markets and provides frequent updates (daily, weekly, and/or monthly) on compliance activities of the Compliance Program. The President of Medicare Markets as well as other senior management are heavily engaged in the Compliance Program and recognize that the Compliance Officer is crucial to protecting the organization and its governing body. The President of Medicare Markets ensures the Compliance Officer is integrated into the organization and has the resources necessary to operate a robust and effective Compliance Program. The President of Medicare Markets receives regular reports of all compliance activities including notices of noncompliance.

E. Changes in Board Composition

The Health Plan will report to the OIG, in writing, any changes in the composition of the Compliance Committee, the Board of Directors, or any actions or changes that would affect the Committee or Board's ability to perform the duties necessary to meet the obligations of the Corporate Integrity Agreement, within 15 days after such a change.

☒ **Freedom Health, Inc.** ☒ **Optimum HealthCare**	**Policy Title: Effective Training and Education** **Primary Department: Compliance** **Policy Number: COMP 03** ☒ **Medicare**
Approved By: _____ _____ Ingrid Velasquez *Date* *Manager, Investigations* Diane E.A. Kortsch 04.30.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date:** 3/28/2012 **Effective Date:** 4/1/2012 **Revision Date(s): 09/01/2012, 05/03/2016, 05/01/2017, 07/31/2017, 01/02/2019, 04/30/2020** **Incorporated former COMP25**
Reference: Medicare Managed Care Manual Chapter 21 – Compliance Program Guidelines and Prescription Drug Benefit Manual Chapter 9 - Compliance Program Guidelines; 42 CFR §§ 422.503(b)(4)(vi)(C), 423.504(b)(4)(vi)(C); The Health Insurance Portability and Accountability Act of 1996 (HIPAA); and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG").	

POLICY:

The Health Plan establishes, implements, and provides effective General Compliance, Fraud, Waste and Abuse (FWA), Health Insurance Portability and Accountability Act (HIPAA), and training and education on the Plan's Corporate Integrity Agreement (CIA), Compliance Program and Federal Health Care Program requirements for every officer, director, associate, volunteer, consultant and Board Members (collectively referred to herein as "Associates)".

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

All covered persons receive at least annual training regarding the CIA requirements, Compliance Program and 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 Plan. Covered persons do not include active Medicare providers who are not employees of the Plan.

General Compliance, HIPAA and FWA Training:

- General Compliance, HIPAA, and FWA training including the Anti-Kickback Statute and the Stark Law are provided within 90 days of initial hiring and annually thereafter for Medicare.
- Annual CIA Requirements

Training completion is tracked via automated reporting and/or signed training attestations.

The training consists of an explanation of the Health Plan's Compliance Program elements, Standards of Conduct and Code of Ethics, CIA requirements, Compliance Policies and Procedures, Fraud, Waste & Abuse and HIPAA definitions, examples, pertinent laws and suspected violation reporting process. Training includes:

- An overview of how to ask compliance questions, request compliance clarification or report suspected or detected non-compliance. Training emphasizes confidentiality, anonymity, and non-retaliation for compliance related questions or reports of suspected or detected non-compliance, HIPAA issues or potential FWA;
- The requirement to report to the sponsor actual or suspected Medicare program non- compliance, 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 re-training 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/process for disclosure of conflicts of interest;
- An overview of HIPAA/HITECH, the CMS Data Use Agreement (if applicable), and the importance of maintaining the confidentiality of personal health information;
- 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/;
- 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 the Compliance designated appointee in a centralized location.

PROCEDURE:

A. New Hire General Compliance Training:

- The Compliance designee develops content as required by Federal and state laws. Content is reviewed at least annually for updates and revisions are approved for use by the Compliance Officer.
- All associate trainings are conducted on a regular frequency (Bi-weekly or as needed). Training is conducted and completed via the on line compliance training system Participant attendance is obtained via completion reports. The following documents are included in the training:

    - Medicare training
    - Compliance Program, FWA, and HIPAA training
    - Compliance Plan and Fraud, Waste, and Abuse (FWA) Prevention Plan
    - Compliance Policies and Procedures
    - CIA Requirements
    - Standards of Conduct and Code of Ethics
    - Reporting Violations Card for display in cubicle or office
    - Reporting mechanisms to report suspected violations
    - Compliance intranet site instructions to locate the above documents

- Once training is complete, new hires complete the online attestation form. The attestation states that the associate will comply with the Health Plan's Compliance Program, Compliance Policies and Procedures and Standards of Conduct and Code of Ethics.
- The completed attestation form is tracked to ensure training has been completed by all associates.

B. Annual Training Process and Procedures

- The Compliance Officer or designee develops content as required by Federal and State laws. Content is reviewed at least annually for updates and revisions and approved for use by the Compliance Officer.
- Annual training is provided via the on-line compliance training system for all permanent, temporary, seasonal associates, and contracted associates. Each person receives an e-mail with the training link. Associates and contractors must complete training and signage of all materials posted to the site. The materials included at a minimum are:

    - Medicare training
    - Compliance Program, FWA and HIPAA training
    - Compliance Plan
    - Compliance Policies and Procedures
    - CIA Requirements
    - Standards of Conduct and Code of Ethics
    - Conflict of Interest

- Each associate and contractor must pass a test on Compliance, FWA, and HIPAA.
- Each associate and contractor must sign an acknowledgement that they have read and will comply with the Health Plan's Compliance Plan, CIA Requirements, Compliance Policies and Procedures and Standards of Conduct and Code of Ethics.
- Certifications of successful completion of the course and a passing score on the test are generated by the on-line system, or paper document when access to compliance training system is unavailable.
- The on-line training system tracks and documents each person's completion of the training. Reports may be generated at any time for documentation purposes.

C. 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 and strategic methods and approaches to conducting oversight of the Organization.

D. Measuring Effectiveness of Training and Education

Effectiveness of the training program is made apparent through compliance with all Medicare Program requirements by all associates 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

E. Records Maintenance

The Health Plan maintains all training records for a period of 10 years, including but not limited to; attendance records, topics, attestations and test scores of tests administered to associates.

☒ **Freedom Health, Inc.** ☒ **Optimum HealthCare**	**Policy Title: Effective Lines of Communication/Disclosure Program** **Primary Department: Compliance** **Policy Number: COMP 04** ☒ **Medicare**
Approved By: Krista Gibbons *Date* *Manager, Delegation Oversight* Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 04/01/2012** **Effective Date: 04/01/2012** **Revision Date(s): 09/01/12, 05/03/2016; 07/05/17, 04/27/2020** **Incorporated former COMP22 & COMP27**
Reference: Medicare Managed Care Manual Chapter 21 – Compliance Program Guidelines and Prescription Drug Benefit Manual Chapter 9 - Compliance Program Guidelines; 42 CFR §§ 422.503(b)(4)(vi)(D), 423.504(b)(4)(vi)(D); The Health Insurance Portability and Accountability Act, (HIPAA) and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG")	

POLICY:

The Plan is committed to conducting business with the highest levels of integrity all while maintaining compliance with all applicable State and Federal Laws, Rules and Regulations and the Corporate Integrity Agreement. The Plan is committed to the timely identification and resolution of all compliance related issues that may adversely impact employees, members and the Organization.

The Plan has established and implemented effective lines of communication to ensure confidentiality and anonymity between the Compliance Officer, board members, business associates, employees, volunteers, consultants and vendors a (collectively referred to herein as "Associates)" as well as the Plan's FDRs (First Tier, Down Stream, and Related Entities).

The 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 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 Plan's Standards of Conduct and Policies and Procedures.

The 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 Plan maintains a separate policy on non-retaliation and non-intimidation to encourage reporting.

The Plan has established the following mechanisms to allow individuals to report any suspected or confirmed violations or non-compliance of the Federal HealthCare Program 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 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, 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, 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
    - **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)
        - PO Box can be used anonymously and confidentially

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 status of the reviews and any corrective action taken.

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 and internal review of the allegations and ensure proper follow 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).

Compliance reports on a quarterly basis to the Compliance Committee and the Board of Directors on the number of hotline cases received, what the primary issues or allegations were and whether the allegations were substantiated.

PROCEDURE:

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

A. Members

The 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. On the Compliance Intranet Page, associates can find, among other things:

- Policies and Procedures
- Compliance and Fraud Waste and Abuse (FWA) Prevention Plan
- Standards of Conduct
- Training (New Hire, Annual Compliance)
- Cubicle Cards, List of reporting mechanisms
- 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 Plan's Compliance Program and dedication to regulatory compliance and business ethics. Various methods of communication are utilized including:

- Posters emphasizing the 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 addresses 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 communications 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 identification and reporting of program noncompliance, FWA and HIPAA concerns.

- Distribution of SOC, training materials, policies and procedures
- Compliance-Provider/Vendor Training System
- Email Communication

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.
- Florida Dept. of Financial Services, Div. of Insurance Fraud: 1-800-378-0445
- Office of Inspector General at HTTP://OIG.HHS.GOV
- Department for Health and Human Services (DHHS): WWW.HHS.GOV/OCR/HIPAA
- Centers for Medicare and Medicaid Services: WWW.CMS.GOV

☒ Freedom Health, Inc. ☒ Optimum HealthCare	**Policy Title: Well-Publicized Disciplinary Standards** **Primary Department: Compliance** **Policy Number: COMP 05** ☒ **Medicare**
Approved By: Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 03/28/2012** **Effective Date: 04/01/2012** **Revision Date(s): 04/01/2016; 07/17/2017; 04/27/2020** **09/01/2012; Incorporated former COMP05, COMP20 & COMP23**
Reference: 42 CFR §§ 422.503(b)(4)(vi)(E), 423.504(b)(4)(vi)(E); 42 CFR 422.2272, 422.2274, 423.2272, 423.2274; CMS Prescription Drug Benefit Manual Chapter 9; Medicare Managed Care Manual Chapter 21;The Health Insurance Portability and Accountability Act (HIPAA) and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG").	

POLICY:

The Plan establishes and publishes disciplinary standards that reflect clear and specific disciplinary policies which promote good faith participation in the Compliance, FWA, Corporate Integrity Agreement, HIPAA and Federal Healthcare Program requirements by officers, directors, employees, volunteers, consultants, (collectively referred to herein as "Associates)" and FDRs (First Tier, Down Stream, and Related Entities).

These standards include policies that:

1. Articulate the Plan's expectations for reporting compliance issues and assist in their resolution.
2. Identify program non-compliance, FWA, HIPAA violations or unethical or illegal behavior; and
3. Provide for timely, consistent, and effective enforcement of the standards when noncompliance, FWA, HIPAA violations or unethical behavior is determined.

PROCEDURE:

A. Publication of disciplinary standards for Associates and FDRs

The Plan publicizes disciplinary standards for Associates and FDRs through various mechanisms.

Associates are notified using the following mechanisms:

- General and Annual compliance training
- Intranet Site
- Posters displayed through employee work areas

FDRs are notified using the following mechanisms:

- Distribution of training material, policies and procedures, and Standards of Conduct
- Compliance-Provider/Vendor Training System
- Provider Manuals
- Email Communication

B. Examples of non-Compliant; FWA; HIPAA; unethical; illegal behavior

Below are a few examples of non-compliant, unethical, and illegal behavior Associates might encounter in their jobs:

1. *Failure to provide medically necessary services*: Fails to provide, to a Plan enrollee, medically necessary items or services that the organization is required to provide (under law or under the contract) to a Plan enrollee, and that failure adversely affects (or is substantially likely to affect) the enrollee.

2. *Marketing Schemes*: When a Sponsor, or its subcontractor, violates the Medicare Marketing Guidelines, or other federal or state laws, rules, and regulations to improperly enroll beneficiaries in a Plan. Examples of such violations include, but are not limited to:
    - Offering beneficiaries, a cash payment as an inducement to enroll;
    - Unsolicited door-to-door marketing;
    - Use of unlicensed agents;
    - Enrollment of beneficiary without their knowledge or consent;
    - Stating that a marketing agent/broker works for or is contracted with the Social Security Administration or CMS;
    - Misrepresents the product being marketed as an approved Plan when it actually is a Medigap policy or non-Medicare drug Plan;
    - Misrepresents the Medicare Advantage or Prescription Drug Plan being marketed (i.e., enrolling Medicare beneficiaries in a MA-PD when they wanted a PDP);
    - Requests financial beneficiary information or check numbers
    - Requires beneficiaries to pay up front premiums.

3. *Improper bid submissions*: The Sponsor inappropriately overestimates or underestimates the bid to manipulate risk corridors and/or payments, including miscalculations of administrative ratio costs within the bids (wrong service lines).

4. *Payments for excluded drugs*: Sponsors must ensure that they only provide coverage for covered drugs.

5. *Multiple billing*: Several payers billed for the same prescription, except as required for coordination of benefit transactions, such as the same prescription being covered and paid for under Medicare Part A or Part B, and then a second time under Part D, and/or possibly Medicaid.

6. *Non-Compendium Payments*: Payments for drugs that are not for a medically accepted indication.

7. *Inappropriate Enrollment/Disenrollment:* Improperly reporting enrollment and disenrollment data to Federal or State agencies to inflate prospective payments.

8. *Appeals process handled incorrectly*: Beneficiary denied their right to appeal or denied a timely appeal.

9. *Adverse selection*: Selecting or denying beneficiaries based on their illness profile or other discriminating factors. The Sponsor may anticipate costs being too high with certain beneficiaries with many or severe comorbid diseases, and improperly acts to expel or refuses to enroll a beneficiary in violation of the regulations or the contract.

10. *False information*: Plan misrepresents or falsifies information it furnishes to an individual under the benefit program.

11. *Delinquent reimbursements*: Beneficiary is not reimbursed by the Plan following retroactive low-income subsidy determination.

12. *Duplicative premiums*: Receiving duplicative co-pays or premiums from beneficiaries.

13. *Excessive premiums*: Imposes enrollees premiums in excess of the monthly basic and supplemental beneficiary premiums permitted under the regulation.

14. *Inaccuracies in eligibility or coordination of benefits*: Inaccurate or incomplete information on eligibility or benefits can lead to wasteful expenditure on drugs.

15. *Inaccurate data submission*: Sponsor submits inaccurate or incomplete prescription drug event (PDE) data.

16. *Catastrophic coverage manipulation*: Sponsors manipulate catastrophic coverage to increase payment by state or federal agencies.

17. *Failure to disclose or misrepresentation of rebates, discounts or price concessions*: Sponsor fails to disclose or misrepresents rebates, discounts, price concessions, or other value added gifts, including concessions offered by pharmaceutical manufacturers.

18. *Bait and switch pricing*: When a beneficiary is led to believe that a drug will cost one price, but at the point of sale the beneficiary is charged a higher amount. This includes frequent formulary changes to induce beneficiaries to sign up for specific drugs that are later removed.

19. *Manipulation of low-income subsidy enrollees:* Sponsor provides false or misleading information regarding the number of its members who have applied for and qualify for the low income subsidy in order to receive unwarranted low income subsidy payments.

20. *Misuse of PHI:* Disclosing HIPAA in an improper manner.

21. *Any conduct that does not follow applicable FWA Laws, Anti-Kickback Statute, Stark Law or False Claims Act.*

Pharmacy:

1. *Inappropriate billing practices*: Inappropriate billing practices at the pharmacy level occur when pharmacies engage in the following types of billing practices:
    - Incorrectly billing for secondary payers to receive increased reimbursement.
    - Billing for non-existent prescriptions.
    - Billing multiple payers for the same prescriptions, except as required for coordination of benefit transactions.
    - Billing for brand when generics are dispensed.
    - Billing for non-covered prescriptions as covered items.
    - Billing for prescriptions that are never picked up (i.e., not reversing claims that are processed when prescriptions are filled but never picked up).
    - Billing based on ―gang visits, (e.g., a pharmacist visits a nursing home and bills for numerous pharmaceutical prescriptions without furnishing any specific service to individual patients).
    - Inappropriate use of dispense as written (DAW) codes.
    - Prescription splitting to receive additional dispensing fees.
    - Drug diversion.
2. *Prescription drug shorting*: Pharmacist provides less than the prescribed quantity and intentionally does not inform the patient or make arrangements to provide the balance but bills for the fully-prescribed amount.
3. *Bait and switch pricing*: Bait and switch pricing occurs when a beneficiary is led to believe that a drug will cost one price, but at the point of sale the beneficiary is charged a higher amount.
4. *Prescription forging or altering*: Where existing prescriptions are altered, by an individual without the prescriber‘s permission to increase quantity or number of refills.
5. *Dispensing expired or adulterated prescription drugs*: Pharmacies dispense drugs that are expired, or have not been stored or handled in accordance with manufacturer and FDA requirements.
6. *Prescription refill errors*: A pharmacist provides the incorrect number of refills prescribed by the provider.
7. *Illegal remuneration schemes:* Pharmacy is offered, or paid, or solicits, or receives unlawful remuneration to induce or reward the pharmacy to switch patients to different drugs, influence prescribers to prescribe different drugs, or steer patients to Plans.
8. *TrOOP manipulation:* When a pharmacy manipulates TrOOP to either push a beneficiary through the coverage gap, so the beneficiary can reach catastrophic coverage before they are eligible, or

manipulates TrOOP to keep a beneficiary in the coverage gap so that catastrophic coverage is never realized.

9. *Failure to offer negotiated prices:* Occurs when a pharmacy does not offer a beneficiary the negotiated price of a drug.

- Billing for services not furnished and/or drugs not provided
- Billing non-covered prescription as covered items
- Billing for expired drugs
- Dispensing without a prescription
- Billing for recycled prescription drugs
- Billing for brand when generics are dispensed
- Altering scripts or data to obtain a higher payment amount
- Misrepresentations of dates, descriptions of prescriptions or services

C. Disciplinary Standards and steps

All disciplinary standards are enforced in a timely, consistent, and effective manner. Records are maintained for a period of 10 years for all violation disciplinary actions, capturing 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 Plan periodically reviews these records of discipline to ensure that disciplinary actions are appropriate to the seriousness of the violation, consistently administered, and imposed within a reasonable timeframe.

The Plan expects all Associates and FDRs to report potential violations of Fraud, Waste and Abuse, Medicare Program non-compliance, and HIPAA. Failing to report violations or the reporting of violations without "good faith" can lead to disciplinary action up to and including termination. The 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 designee, will notify the employee or FDR to bring attention to the existing performance/compliance issue. The Compliance Officer, or authorized designee, informs the employee or FDR the nature of the problem or compliance violation. The Compliance Officer, or authorized designee, clearly outlines expectations and steps the employee or FDR must take to improve performance or resolve the problem. As a result of that discussion, both the Compliance Officer, or authorized designee, and the employee/FDR 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 to the employee or FDR.

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

Step 3: Extension of Written Warning or Termination

If the FDR's or Associate performance/compliance issue does not improve sufficiently, the Compliance Officer, or authorized designee, may decide to extend the CAP/PIP for a limited period – if the severity of the compliance violation is low risk.

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

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

☒ Freedom Health ☒ Optimum HealthCare	**Policy Title: Effective System for Routine Monitoring, Auditing, and Identification of Compliance Risks** **Primary Department: Compliance** **Policy Number: COMP 06** ☒ **Medicare**
Approved By: Monique S. Akins 4.27.2020 Monique Akins *Date* *Manager, Compliance* Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Staff VP Compliance* *Date*	**Create Date: 03/28/2012** | **Effective Date: 04/01/2012** **Revision: 09/01/2012; 10/29/2013; 05/6/2016; 04/12/2017; 07/18/2017; 12/14/2018; 04/27/2020** 03/28/2012 – Replaces previous policy #s: COMP02, COMP05, COMP19, COMP21, COMP24, COMP29
Reference: 42 CFR §§ 422.503(b)(4)(vi)(E), 423.504(b)(4)(vi)(E), 42 CFR §§ 422.503(b)(4)(vi)(F), 423.504(b)(4)(vi)(F), 422.504(e)(2), 423.505(e)(2), Prescription Drug Benefit Manual Chapter 9 Medicare Managed Care Manual Chapter 21; and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG").	

POLICY:

The Plan performs a comprehensive annual risk assessment and conducts an ongoing review throughout the year to identify and address risks associated with the plan's participation in Federal Health Care Programs and the Corporate Integrity Agreement. The Plan develops and implements monitoring and audit work plans based upon the results of the risk assessment. Corrective Action Plans are implemented and tracked to mitigate all Organizational risks.

The Compliance Officer, Executive Management, Compliance Committee, and Board of Directors 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, third party independent consultants, 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 and Medicaid regulations, sub-regulatory guidance, contractual agreements, all applicable federal and state laws, as well as the Plan's policies, protecting against Medicare and Medicaid program noncompliance, HIPAA and potential FWA. The monitoring and audit results are reported to the CEO, Compliance Committee, and the Board of Directors at least quarterly.

The Plan has developed a strategy to monitor and audit its FDRs to ensure they are in compliance with applicable laws and regulations. The Plan's contractual arrangements with first tier entities provide for routine and random auditing; *please reference the Conducting Oversight of First Tier, Downstream and Related Entities (FDRs) Policy and Procedure for additional details.*

PROCEDURE:

Risk Assessments, Monitoring and Audit Work Plan, and Corrective Actions

An effective monitoring and auditing program began with a comprehensive internal risk assessment. In order to establish an effective system for monitoring and auditing, the Plan utilizes a Risk Assessment Tool that takes into account operational areas. The Plan's operational areas are assessed for potential and inherent compliance issues (including noncompliance, FWA, HIPAA). The Plan performs a comprehensive annual risk assessment and conducts an ongoing review throughout the year to identify and address risks associated with the Plan's participation in Federal Health Care Programs. An FDR risk assessment is done independent of plan's operational risk assessment and is based on plan's FDR oversight policy

Due to high propensity of risks, the following areas are evaluated for risks (not an exhaustive list): Sales and Marketing (inclusive of agent/broker activities), Enrollment/Disenrollment, Credentialing, OIG/GSA exclusion verification, Quality Assessment, Appeals and Grievance, Benefit/Formulary Administration, Claims, Provider Network, Medical Risk Management, and FDR functions. Next, identified issues are prioritized based on which risk area will have the greatest impact on the Plan's Compliance Program including all regulations associated with the plan participation in the Federal Health Care Programs. The following risk levels are utilized to prioritize the risks:

High	Occurs when a practice, process or procedure has been identified as non-functional/non-productive, noncompliant and/or has high impact risk organizationally or to a beneficiary.
Medium	Occurs when an issue, process, etc. has been remediated; however, the issue, process, etc. poses a potential impact compliance risk, organizationally or to the beneficiary.
Low	Occurs when risk results from new state/federal regulatory guidance that has been released or the risk identified is a minimal impact compliance risk, organizationally or to the beneficiary.

The Risk Assessment results are reviewed with Executive Management and presented at least quarterly to the Compliance Committee and Board of Directors. Based on the Risk Assessment the Compliance area develops auditing and monitoring work plans. The risk assessment results are used for the development of the monitoring and auditing work plans. Next, the Compliance area implements these work plans in the areas of identified risks. Further, Corrective Action Plans are implemented and tracked to ensure all risks have been mitigated. The monitoring and audit work plan process is further described in detail below.

Monitoring Process

Monitoring activities are regular reviews performed of the Plan's internal operational areas to confirm ongoing compliance and to ensure that corrective actions are undertaken and effective when issues are detected. The Monitoring Work Plan consists of the department monitored, date monitoring efforts began, scope of monitoring activity (what is being measured and for what timeframe), type of monitoring conducted (report analysis and/or sample reviews), description of findings and outcome of monitoring efforts, including a description of any corrective/remediation action taken as a result of the finding. The Monitoring Work Plan schedule is organized by quarter.

1. Monitoring at the area level (including Compliance) may consist of either report analysis and/or sample validation.
    a. Report Analysis – Examination of reports generated during the normal course of operations to ensure performance & compliance metrics are met.
    b. Sample validation - Examination of correspondence and notations related to monitoring activity to ensure compliance is met.
2. Once the analysis and/or validation of the activity is complete, each area is required to report their results to Compliance. Areas must ensure that any activity found to be non-compliant includes documented corrective actions and/or plans for remediation upon submittal to Compliance.
3. Once reports have been submitted, the Compliance Team will track, review, and report on the receipt of the monitoring report. If warranted, additional corrective actions or Corrective Action Plan (CAP) may be issued based upon compliance recommendations. All Corrective Action Plans are tracked, monitored, and validated by the Compliance Department to ensure remediation is sufficient. Activities with Corrective Action Plans are incorporated on the risk assessment.
4. Based upon the monitoring activity results, compliance may add monitoring activity to the audit work plan to validate and close out monitoring activity; or add to the risk assessment for continued monitoring.
5. Monitoring updates and results are shared with the Compliance Committee, the CEO, Sr. Leadership, and the Plan's Governing Body.

Audit Process

Audit activities are formal reviews performed of the Plan's 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 Audit Work Plan includes the department being audited, activity audited, audit objectives/scope, audit type (announced vs. unannounced, desk audit vs. onsite, internal vs. external), audit schedules (including start and end dates), audit status (scheduled, open or closed), audit findings/outcomes, as well as a description of any corrective/remediation action taken as a result of the findings.

Compliance conducts announced and unannounced audits on operational areas. Announced audits are audits in which the operational area has been made aware of the audit schedule in advance (via Compliance Committee or Sr. Management reporting). Unannounced audits occur when no

notification is provided to the operational area via the audit announcement as an indication of impending audit activity. Unannounced audits may be conducted for various reasons, such as feedback from executive bodies, regulatory bodies, letters of noncompliance, etc.

Compliance audits are conducted utilizing the following methodology:

1. Audit planning

    a. Audit activity selected based on audit work plan.
    b. Outline compliance and/or operational requirements
    c. Review guidance specific to audit event
    d. Customized audit based on, but not limited to, risk criteria, such as new or updated regulatory guidance, organizational or industry trends, reports of compliance issues, etc.
    e. Draft audit notification – Notice should include, but is not limited to, the following: activity audited, audit objectives/scope, universe specifications and due date for universe data, and any other required documentation (policy & procedures, step actions).

2. Opening Conference/Meeting (as warranted by compliance)

    a. Discuss proposed audit plan and objectives
    b. Discuss processes, acquire contacts, and known areas of risks/issues
    c. Finalize audit plan and objectives (*if applicable*), and resubmit to contact

3. Initiate Audit/Perform Fieldwork

    a. Send out the audit notification
    b. Analyze the universe and select samples
        i. Samples are selected based on aberrant behavior, targeted sampling, or statistically valid methodology.
        ii. Upon identification of deficiencies and/or completion of audit exercise, notify operational area business owner.
        iii. Notification may be provided verbally and/or in writing when a potential compliance risk is identified. Non-compliance notification is provided to the business owner in writing.
        iv. Identified deficiencies may result in one of the following:

            1. Corrective Action Plan (CAP) –

               Immediate Corrective Action Required (ICAR) - An ICAR is the result of non-compliance with specific requirements that has the potential to cause significant beneficiary harm.

               Corrective Action Required (CAR) - A CAR is the result of a material non-compliance with specific requirements that does not have the potential to cause significant beneficiary harm.

2. Observations

   Observations- Observations are either immaterial events of non-compliance with specific requirements or other items that may be useful to management in preventing contract non-compliance in the future (i.e. isolated human error). Observations may require follow up actions.

4. Prepare Draft Audit Report

   a. Document the audit results in an audit report which includes: the audit objective, scope and methodology, findings, and corrective actions, if issued.
   b. The approved draft audit report is presented for review & acceptance or rebuttal to the business owner (including CAP document or request corrective actions when appropriate).

5. Prepare Final Audit Report

   a. Upon receipt and review of the business area response to the approved draft report, Compliance prepares the final audit report, inclusive of the audited area's response and CAP remediation.
   b. The Compliance approved final audit report is submitted to the audited area and applicable senior management

6. Close Audit

   a. Internal audit and CAP documents are updated
   b. Required follow-up reviews are added to audit/monitoring schedule
   c. Audit results are presented to the Compliance Committee and Board of Directors on a quarterly basis.

7. Follow-Up Review

   a. An auditor performs the CAP validation review/Follow-up review on the audit work plan. The audit line on the Work Plan will track the audit through CAP closure, documenting significant dates, including, but not limited to the date the initial audit closed, date CAP notification provided, and dates initial and final remediation completed.
   b. For remediated deficiencies, Compliance will approve and close the CAP on the CAP Tracker.
   c. For non-remediated deficiencies, Compliance will require additional monitoring/auditing until the deficiency is remediated.

Tracking and Documenting Compliance efforts

The Plan tracks and documents all internal monitoring and auditing activity and compliance efforts. The Monitoring and Auditing 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.

Compliance tracks and documents corrective actions with business area leaders. Business area(s) provide Compliance with a CAP document which includes a root cause analysis (RCA), Impact analysis (IA), and remediation actions based on RCA and IA. A Compliance review is conducted to determine if appropriate remediation actions have been taken to correct the deficiency and sustain compliance.

Regularly, the Monitoring and Auditing 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 CEO, Compliance Committee, and BOD.

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 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.

☒ Freedom Health ☒ Optimum HealthCare	**Policy Title: Procedures and System for Prompt Response to Compliance Issues** **Primary Department: Compliance** **Policy Number: COMP 07** ☒ **Medicare**
Approved By: Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Staff VP Compliance* *Date*	**Create Date: 3/28/2012** **Effective Date: 04/01/2012** **Revision Date(s): 04/01/2012; 09/01/2012; 04/01/2016; 04/12/2017; 07/17/2017; 11/12/2019; 04/27/2020** - Replaces former COMP03 & Incorporates former COMP05
Reference: CMS Prescription Drug Benefit Manual Chapter 9; Medicare Managed Care Manual Chapter 21; 42 CFR §§ 422.503(b)(4)(vi)(G), 423.504(b)(4)(vi)(G), PPACA § 6402(d)(2), 63 Fed. Reg. 58,399 (1998); The Health Insurance Portability and Accountability Act, (HIPAA); and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG").	

POLICY:

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

When the Plan 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 and implements appropriate corrective actions in response to any confirmed violations.

The Plan also has procedures to voluntarily self-report potential program non-compliance, HIPAA, or fraud violations to appropriate state and federal regulatory agencies.

PROCEDURE:

A. Conducting a Timely Reasonable Inquiry of Detected Offenses

The Plan's Compliance area conducts a timely and well-documented reasonable inquiry into any potential non-compliance, HIPAA, or FWA violations. The potential violation may be discovered through a hotline, a website, an enrollee complaint, during routing monitoring or self-evaluation, an audit, or by regulatory authorities. Regardless of how the potential violation is identified, the issue is recorded in the disclosure log within two days, then a reasonable inquiry is initiated as quickly as possible, but no later than two weeks after the date the potential incident was identified.

1. The Inquiry is officially initiated once recorded in the Compliance/Disclosure log (including dates, source of investigation, issue type, corrective action, and closure date). All Inquiries will initiate an investigational review by the Compliance Officer and/or their designee;
2. The investigational research efforts include, but are not limited to:
    - Collection of the facts
    - Review of regulatory guidance
    - If required, contact with members, and/or providers
    - Data analysis of the issue
    - If required, meeting with area leaders and senior management
3. Confidentiality is maintained by minimizing the number of people privy to investigational information. Information is only shared with applicable parties;
4. If warranted, corrective action plans are issued.
5. If warranted, members, providers, regulatory bodies, and/or other parties are notified of the issue. Once all appropriate parties are notified the case is closed.

B. 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 non-compliance. 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.

Follow up is done on all corrective actions 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 employee or contract.

Documentation is maintained on all deficiencies identified and corrective actions taken.

C. Procedures for Self-Reporting Potential Fraud, HIPAA, or Non-Compliance

The organization has developed a process to voluntarily self-report FWA, HIPAA, and program non-compliance as it believes it's an important component of maintaining an effective compliance program. Self-reporting can be done through various mechanisms, such as, but not limited to: third party hotline (phone & web); secured email, direct communication with Compliance leadership (phone, email, and/or in person). Self-reporting can be made anonymously and should always be done in good faith.

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

For Medicaid, all suspected or confirmed instances of internal and external fraud and abuse relating to the provision of and payment for Medicaid services including, but not limited to, Plan employees/management, providers, subcontractors, vendors, delegated entities, or enrollees under state and/or federal law be reported to the Agency for Health Care Administration's Bureau of Medicaid Program Integrity (MPI) within fifteen (15) calendar days of detection. Additionally, any final resolution reached by the Plan shall include a written statement that provides notice to the provider or enrollee that the resolution in no way binds the State of Florida nor precludes the State of Florida from taking further action for the circumstances that brought rise to the matter.

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

☒ **Freedom Health, Inc.** ☒ **Optimum HealthCare**	**Policy Title: Special Investigation Unit/Fraud, Waste & Abuse Policy** **Primary Department: Compliance - SIU** **Policy Number: COMP 08** ☒ **Medicare**
Approved By: Ingrid Velasquez *Date* *Manager, Investigations* Diane E.A. Kortsch 05.04.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 5/15/2013** | **Effective Date: 5/15/2013** **Revision Date(s): 12/1/2010; 3/1/2011; 5/15/2013 - replaces previous SIU SOP 2; 11/5/2015, 05/11/2016, 09/21/2016, 04/10/2017; 12/05/2017; 12/15/2017, 08/16/2018, 11/07/2018, 05/04/2020**
Reference: Medicare Improvements for Patients and Providers Act of 2008 (MIPPA); The Prescription Drug Benefit Manual for Part D – Chapter 9; Medicare Managed Care Manual Chapter 21 – Compliance Program Guidelines; F.S 42 U.S.C. §1320a-7a; 42 U.S.C. §1395nn; 18 U.S.C. §1347; 18 U.S.C.§1035; 18 U.S.C. § 286, §287; 18 U.S.C. §1001; 18 U.S.C. §669; 18 U.S.C. §1518; 18 U.S.C. §371; 18 U.S.C. §1956; §1961 et. Seq, 42 U.S.C. §1320a-7b(b); 42 U.S.C. 1395 §1877; 42 U.S.C. § 1320a-7a; State Specific False Claims Acts; 31 USC 3729-3733; 42 USC 1320a-7b(b); The Health Insurance Portability and Accountability Act of 1996 (HIPAA), 409.91212, F.S., 42 CFR 438.608; and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG").	

POLICY:

The Plan is committed to comply with applicable federal and state laws, rules and regulations related to fraud, waste and abuse and the Corporate Integrity Agreement ("CIA") The Plan has created and fully supports a Special Investigation Unit (SIU), and has given this unit primary responsibility for the detection, prevention, investigation, reporting, correction and deterrence of Fraud, Waste and Abuse (FWA). The SIU unit will report to the Compliance Officer (CO), and accordingly, will maintain clear lines of communication with the CO at all times. The SIU will maintain written policies, procedures, and adhere to standards of conduct that articulate the Plan's commitment to comply with all applicable federal and state standards.

The SIU will promote the immediate reporting of suspected incidents of FWA by establishing clear lines of communication with employees, business associates and downstream entities. The SIU will assist in supporting and enforcing established Plan compliance standards which are clearly communicated through publicized disciplinary guidelines. The SIU will immediately report, as defined by state and federal guidelines, all suspected or confirmed incidents of FWA, and will assist state and federal investigative agencies on FWA investigations upon request.

Definitions:

Fraud is knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program or to obtain (by means of false or fraudulent pretenses, representations, or promises) any of the money or property owned by, or under the custody or control of, any health care benefit program. 18 U.S.C. § 1347.

Waste is the overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare program. Waste is generally not considered to be caused by criminally negligent actions but rather the misuse of resources.

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

Inquiry is any request for information from a regulatory Agency, Law Enforcement agency or any other entity for review and/or investigation. Once the inquiries are researched and found to have exposure to the Plan, the inquiries are transitioned to FWA cases.

Overpayment includes any amount that is not authorized to be paid by the Medicare program whether paid as a result of inaccurate or improper cost reporting, improper claiming, unacceptable practices, fraud, abuse, or mistake.

Case is any confirmed Fraud, Waste and Abuse complaint or incident by a provider, member or employee.

FWA is Fraud, Waste and Abuse.

Special Investigations Unit (**SIU)** is an internal investigation unit responsible for conducting investigations of potential FWA.

Role of the SIU:

The Plan has established a SIU to develop and implement a comprehensive anti-fraud program to prevent, detect, investigate, resolve, correct and report incidents of suspected fraud, waste and abuse. While the SIU is the primary investigative unit concerning suspected fraud, waste and abuse, the FWA program is not limited to those designated personnel. The SIU will assist management in meeting compliance standards regarding fraud, waste and abuse and will serve as liaison between the Plan, providers, contractors, Federal and State agencies, and other constituents in the prevention, detection, and reporting of any suspected fraud waste and abuse.

SIU areas of responsibility may include:

- Reducing or eliminating Medicare Part C and D benefit cost due to FWA
- Reducing or eliminating fraudulent or abusive claims paid for with federal dollars
- Preventing illegal activities
- Identifying enrollees with overutilization issues
- Identifying and recommending providers for exclusion, including those who have defrauded or abused

the system to the appropriate regulatory agency and/or law enforcement
- Referring suspected, detected or reported cases of illegal drug activity, including drug diversion to the appropriate regulatory agency and/or law enforcement and conducting case development and support activities for the appropriate regulatory agency and law enforcement investigation
- Assisting law enforcement by providing information needed to develop successful prosecution

The SIU will develop and maintain a comprehensive set of Policy and Procedures and will incorporate changes as needed based on state, federal, or plan mandates.

Company Internal Structure and Communication Pathway:

The SIU reports directly to the Compliance Officer (CO). The CO reports to the President of Medicare Markets America's First Choice (AFC) and the Board of Directors. The Compliance Officer has unrestricted access to the health plan's governing body for compliance reporting, including fraud, waste and abuse and will maintain effective lines of communication with the health plan's employees. The Compliance Officer and/or the SIU Manager reports, on a quarterly basis, all FWA activity to the Compliance Committee. The same information also goes to the Board of Directors on a quarterly basis.

Conformance to State and Federal Requirements:

The Plan is required to comply with applicable statutory, regulatory, and other requirements, sub-regulatory guidance, and contractual commitments related to Medicare including Medicare Part D benefits.

The Plan's Anti-Fraud Program has been designed in accordance with, but not limited to:
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Federal and State laws pertaining to the Medicare Programs
- The Medicare Anti-Kickback Statute (42 USC 1320a-7b)
- The False Claims Act (31 USC 3729-3733)
- State Specific False Claims Acts
- The Deficit Reduction Act of 2005
- Medicare Improvements for Patients and Providers Act of 2008 (MIPPA)
- The Prescription Drug Benefit Manual for Part D – Chapter 9
    - Civil Monetary Penalties Act (42 U.S.C. §1320a-7a)
    - Ethics in Patient Referrals Act of 1989 (42 U.S.C. §1395nn)
    - Health Care Fraud (18 U.S.C. §1347)
    - Criminal False Statements Related to Health Care Matters (18 U.S.C.§1035)
    - Criminal False Claims Act (18 U.S.C. § 286, §287)
- Criminal False Statement Act (18 U.S.C. §1001)
- Theft or Embezzlement in Connection with Health Care (18 U.S.C. §669)
- Obstruction of Criminal Investigations of Health Care Offenses (18 U.S.C. §1518)
- Criminal Conspiracy (18 U.S.C. §371)
- RICO and Money Laundering Acts (18 U.S.C. §1956, §1961 et. seq.)
- Federal Anti-Kickback Act (42 U.S.C. §1320a-7b(b)) and Anti-Kickback Act of 1974
- Stark Law (42 U.S.C. 1395nn §1877)
- Beneficiary Inducement Civil Monetary Penalty Law (42 U.S.C. § 1320a-7a)
- All other applicable Federal and State statutory, regulatory, and contracted requirements

I. Prevention and Detection:

As a component of the Plan's Compliance Program, the SIU utilizes a multi-faceted approach to prevent and detect suspected or potential FWA, involving both pre-payment and post-payment claims edits/strategies. The

SIU utilizes a combination of analytical tools, clinical expertise, investigative knowledge, internal and external referrals, and will also depend on an effective education and awareness training program to maximize employee, business partner and downstream entity referrals.

The SIU will proactively search for potential FWA using a specialized targeted approach.
In addition, through clear lines of communication, the SIU will establish multiple avenues to allow employees, business partners and downstream entities to report suspicious or potentially fraudulent activity. Partnership with federal agencies and will open up intelligence avenues and information sharing protocols to enhance our overall prevention and detection capability.

Compliance Policy COMP 04 identifies methods of availability for all reporting of suspected or confirmed fraud, waste and abuse, HIPAA, or other compliance concerns when they are identified.

One of the key components of SIU's ongoing activities is the data mining of the claims payment system to: 1) validate elements of claims are billed in accordance with standardized billing practices; 2) ensure claims are processed accurately; and, 3) ensure payments reflect the service performed as authorized.

Some of these claim edits are listed below:

- Duplicate Claim Submission
- Members eligibility at time of service
- Non covered services
- Services requiring prior authorizations
- Services requiring specific modifiers
- Invalid procedure or diagnosis codes
- Unbundled procedures
- Incidental procedures
- Exclusive procedures
- Diagnosis and/or Procedure code with gender mismatch
- New patient code billed for established patient
- Global pre/post codes billing within the global period
- Procedure code not typical with patient age/gender
- Typical cosmetic procedure
- Place of service with procedure code mismatch
- Multiple procedure reductions

The Plan's PBM - Pharmacy Fraud
The Plan's Pharmacy Benefit Manager (PBM) utilizes 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

Utilization Fraud
When detected, SIU receives FWA reports from the UM department in regard to the following suspicious fraud, waste and abuse activities:

- Hospice Eligibility
- Overlapping Dates of Services
- Hospital Acquired Conditions (HAC)
- Never Event
- Durable Medical Equipment (DME) / intravenous (IV) Therapy
- High Producing, High Cost Providers
- Questionable Member Eligibility
- Inpatient vs. Observation

SIU also utilizes the UM department upper management for confidential medical records review.

Sales/Marketing
The Compliance area works closely with our Sales& Marketing area to prevent FWA. If either team identifies any concerns/issues surrounding FWA, the concern will be forwarded to SIU for investigation. Such as the following:

- Member complaints on agents
- CMS complaint tracking module
- Grievance department logs
- State agency referred cases

Claims
The 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

The claims area refers cases to SIU when a member contacts the plan advising care was not received. Medical records are also referred to SIU for providers that are flagged for possible fraudulent behavior.

Health Services
The plan's Health Services department may identify scenarios during authorization and utilization reviews indicating 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 to SIU any cases where Fraud, Waste or Abuse may be identified.

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

Finance
The Plan's Finance department incorporates various internal controls to identify Fraud, Waste or Abuse.

Member Services
The Plan's Member Services department refers instances of member's allegations of Fraud, Waste or Abuse.

Appeals & Grievances
The Plan's Appeals & Grievances department refers instances of member allegations of Fraud, Waste or Abuse.

PROCEDURE:

FWA Investigation Procedure:

All incidents of suspected FWA will be thoroughly reviewed by SIU personnel and logged into the Plan's case tracking system as a case (lead), or inquiry upon receipt. SIU investigators will evaluate the information and perform a series of investigative steps which are designed to collect facts and establish a basis for resolving the case (lead) or inquiry. Cases will be investigated to resolution and all files will be maintained in the Plan's case tracking system.

The SIU is responsible for the following:

- Screening all reports of suspected fraud, waste and abuse
- Establishing a file for each case or inquiry of known or suspected fraud, waste or abuse detected
- Obtaining necessary supporting documentation for all case files, which may include copies of medical records, member applications, correspondence, policies, medical bills and claim forms, corporate records, background reports, and other relevant documents
- Conducting investigations to conclusion in accordance with the procedures established by the SIU
- Educating and correcting providers, institutions, and/or business partners on proper billing codes and/or procedures when FWA is identified
- Coordinating with the Compliance Officer and/or Legal Department during the course of an investigation as needed

Investigations consist of performing the extended procedures necessary to determine the occurrence of potential FWA activities as suggested by scheme indicators, facts, and evidence. The investigative process includes gathering and verifying sufficient information in order to determine whether or not evidence suggest that fraud waste or abuse may have been committed.

Upon receipt of information relating to suspected FWA, the SIU personnel will gather the initial data and open a case (lead) or inquiry in the case tracking system. Investigative staff will record the date of receipt, day, time in, description of the allegation, additional details or comments complainant or source of the lead, the parties involved, the state of occurrence, the county of occurrence, the Line of Business (LOB), investigator assigned, and will copy all related documents into the case tracking system or case file. The documents will be collated into the corresponding case file, which will be organized to unit standards and maintained in accordance with

HIPAA standards as well as the Plan's Compliance Program. The case files will be annotated with the case ID and stored in locked filing cabinets, again in accordance with HIPAA standards.
After opening an inquiry/case (lead), SIU investigators will complete what is referred to as SIU "Preliminary Due Diligence", which includes the collection of information that will assist SIU personnel in formulating an action plan or closing the case (lead) or inquiry as unfounded.

During the course of the investigation, several other avenues may develop requiring additional information.

After performing due diligence on a case (lead) or inquiry, the investigator must assess the findings and determine if the case is suspicious. When the investigation cannot rule out the allegation or concern as unfounded, the SIU shall consider the case or (lead) inquiry to be suspicious.

If, after performing 'Preliminary Due Diligence', the investigator is able to declare the allegation or concern as unfounded, and has made a good faith effort in making this determination, the inquiry/case (lead) should be closed, and the notes in the file should reflect the reason for making the determination. The case file will be maintained in accordance with state and federal regulations, allowing investigative staff to re-open any case (lead) or inquiry that was previously closed if necessary.

Once a case has been determined to be a suspected FWA, an action plan, will be developed to progress the investigation toward resolution. Additional investigative steps may include, but are not limited to, member interviews, requests for medical records, clinical expertise related to episode treatments, information and intelligence gathering, random or targeted sampling of medical charts, on site audits, coordination with state and federal agencies and coordination with delegated vendors and business partners.

As the case scope develops, a notice may be sent out to the appropriate departments and personnel, informing those personnel that the SIU intends to contact the provider, member, institution, or agency. The SIU will diligently pursue all FWA leads in accordance with state and federal regulation.

A request for information, which may include requests for medical records, financial data, member information, or administrative data, will be sent to the appropriate party. The SIU will utilize either US Postal Registered Mail, or a Company approved shipping service. Upon confirmation of receipt, the investigator will document the case files accordingly.

Providers or members that are unwilling to provide the requested data to the SIU may prompt the need to either involve the provider relations representatives or legal counsel in resolution. The Compliance Officer has the final determination on next steps if resolution cannot be reached and the member or provider refuses to comply.

SIU leadership will determine how to proceed with the investigation once the data has been received.

Unfounded
Once the investigation is complete and the findings have been determined, the resolution of the case may result in the allegation being unfounded. The investigator will document the findings and summarize the reasoning for the determination. The case will be closed and the records will be retained in accordance with state and federal regulations.

Correction & Education
Once the investigation is complete and the findings have been determined, the resolution of the case may result in the need to educate the provider and correct the errors or issues which caused the investigation. Through coordination and explanation, the correction can be made and thus resolving the concern. Often these are caught early on an inquiry and resolved at that point. Education may be appropriate to resolve investigations as well and would involve the explanation or clarification of guidelines or regulations, and allows the provider to correct the errors that caused the concern. This often occurs in the selection of the Current Procedural Terminology

(CPT) codes or the International Classification of Disease, Ninth & Tenth Edition (ICD-9; ICD-10) codes or successor that was used to determine payment.

Recovery

If an overpayment is determined, the investigator will draft the response to the Provider or member and will enter the amount determined to be overpaid in the SIU tracking system. A refund request letter will be sent to the Provider or member and recorded in the SIU tracking system.

Prior to sending the Overpayment letter, the investigator may send a notice out to the appropriate departments and personnel, informing those personnel that the SIU intends to contact the Provider, member, institution, or agency and request a refund.

SIU will monitor and record the overpayment in the SIU tracking system. If the overpayment refund request is not received in a timely manner, (generally 30 days), the Investigator will submit a second request for refund by registered mail. If there is no response by the Provider or member within 30 days of the request, SIU may refer the overpayment request to the Claims department and/or Legal department for further action.

Settlement or Litigation

Once the investigation is complete and the findings have been determined, the resolution of the case may result in a settlement or litigation. The provider or member has the opportunity to explain, refute or mitigate any determination made by the SIU, and the Plan will carefully consider all facts. This may result in a teleconference or meeting in an attempt to resolve the issue identified. Each case is unique and will require different steps based on results of the investigation. The SIU will not approve any offer for settlement without consultation with leadership. If state or federal agencies are involved in the investigation, or choose to determine next steps, the Plan will cooperate fully and shall not impede with those efforts.

Investigators will work diligently to resolve and finalize the investigations, including the development of corrective action. If a resolution cannot be reached, or if the facts of the case confirm fraudulent or abusive activity, the Plan is to immediately inform the appropriate state or federal agency as dictated by licensure and may result in case litigation. This may include the building of formal evidence packets, being deposed, testifying in court, working with federal or state agencies, and or presentations to senior management. The Plan may choose to utilize external Legal representation and/or to request state or federal support. The Compliance Officer has the final authority in making this determination, if needed.

Corrective Action Plan

The Health Plan corrects 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 may be issued. The corrective action is designed to correct the underlying problem that resulted in program violations and to prevent future noncompliance. The corrective action may also have timeframes for specific achievements towards addressing the deficiency. For contractors, detailed ramifications are also listed in the written agreement if the contractor fails to implement the corrective action satisfactorily.

A follow up is done on all corrective action 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 employee or contract. Documentation is maintained on all deficiencies identified and corrective actions taken.

Record Retention

Records will be maintained in accordance with state and federal regulations and will be produced upon request to appropriate authorities. In accordance with HIPAA regulation, all data will be maintained to protect the privacy and integrity of the information. The SIU will archive materials as needed and will record the tracking information to include case identification.

II. **Reporting:**

The Plan's SIU area will report suspected or confirmed cases of Medicare Fraud, Waste and Abuse activities to the MEDIC and/or the appropriate law enforcement agency as described below:

1. **CMS & HHS-OIG:**
   The Medicare Advantage (MA) Organization agrees to comply with applicable Federal laws and regulations designed to prevent fraud, waste and abuse, including, but not limited to applicable provisions of Federal criminal law, the False Claims Act (31 U.S.C. 3729), and the anti-kickback provision of section 1128B of the Social Security Act; HIPAA Administration Simplification Security and Privacy Rules at 45 CFR Parts 160, 162, and 164; and Section 6032 of the Federal Deficit Reduction Act of 2005; and all other applicable Federal statutes and regulations.

2. **Other Reporting:**
   The Health Plan shall provide a copy of any corrective action required by federal governmental entities within thirty (30) calendar days after execution of such plans.

   a) **Office of Inspector General**

   Office of Inspector General
   U.S. Department of Health & Human Services
   Attn: HOTLINE
   P.O. Box 23489
   Washington, DC 20026
   www.oig.hhs.gov
   Email: HHSTips@oig.hhs.gov
   Phone: 1-800-HHS-TIPS (1-800-447-8477) or TTY 1-800-377-4950
   Fax: 1-800-223-8164 (10 pages or less)

   b) **State Division of Insurance Fraud**

   Florida

   Department of Financial Services, Division of Insurance Fraud
   Bureau of Crime Intelligence and Analytical Support
   200 E. Gaines Street
   Tallahassee, FL 32399-0324
   Phone: 1-800-378-0445
   https://apps8.fldfs.com/first/

   c) **Investigations Medicare Drug Integrity Contractor (I-MEDIC)**
   If after conducting a reasonable inquiry by the SIU, it is determined that potential fraud or misconduct related to the Parts C and D Medicare program has occurred, the conduct should be referred to the Investigations Medicare Drug Integrity Contractor (I-MEDIC) promptly, but no later than 30 days after the determination that a violation may have occurred.

   Once it is determined that a referral should be made to the I-MEDIC, the plan will develop a referral package that includes, to the extent available, the following:
   - Provider name, all known billing and tax identification numbers, and addresses
   - Type of provider involved in the allegation and the perpetrator, if an employee of the provider

- Type of item or service involved in the allegation
- Place of service
- Nature of the allegation(s)
- Timeframe of the allegation(s)
- Narration of the steps taken and information uncovered during the Sponsor ‘s screening process
- Date of Part D service, drug code(s)
- Beneficiary name, beneficiary Health Insurance Claim (HIC) number, address and telephone number
- Name and telephone number of the Sponsor employee who received the complaint
- Contact information of the complainant, if not the beneficiary
- All documents pertaining to prior sanctions and/or compliance history and corrective actions taken, if any

If the I-MEDIC requests additional information the Plan shall furnish the requested information within 30 days, unless the I-MEDIC otherwise specifies. In some rare instances, there may be a need to acquire information in less than 30 days, e.g., in case of risk to patient health.

d) **Office of Diversion Control**
The plan shall complete the Office of Diversion Control methods of reporting Part D suspected Fraud through the following online link http://www.deadiversion.usdoj.gov/Reporting.html

e) **Florida Medical Quality Assurance (Licensing Board)**
The plan shall complete the Healthcare Provider Complaint Form through the following online link http://www.floridahealth.gov/licensing-and-regulation/enforcement/_documents/complaint-form-20152.pdf
Consumer Services Unit
4052 Bald Cypress Way, Bin C-75
Tallahassee, FL 32399-3275
Email: mqa.consumerservices@flhealth.gov
Fax: (850) 488-0796

f) **Reporting**

1. The Health Plan shall report all suspected or confirmed instances of provider or recipient fraud or abuse within 15 calendar days after detection to the Office of Medicaid Program Integrity within the agency. At a minimum the report must contain the name of the provider or recipient, the Medicaid billing number or tax identification number, and a description of the fraudulent or abusive act. The Office of Medicaid Program Integrity in the agency shall forward the report of suspected overpayment, abuse, or fraud to the appropriate investigative unit, including, but not limited to, the Bureau of Medicaid program integrity, the Medicaid fraud control unit, the Division of Public Assistance Fraud, the Division of Investigative and Forensic Services, or the Department of Law Enforcement.

2. **Mandatory or Permissive Exclusions**
The Health Plan will disclose to DHHS OIG, with a copy to MPI within twenty (20) working days after discovery, the identity of any person who has ownership or control interest in the Health Plan, or is an agent or managing employee of the Health Plan;

i. Has been convicted of a criminal offense related to that person's involvement in any program under Medicare, Medicaid, or the Title XX services program since the inception of those programs;
ii. Has been denied initial entry into the Health Plan's network for program integrity-related reasons; and/or;
iii. Is a provider against whom the Health Plan has taken any action to limit the ability of the provider to participate in the Health Plan's provider network, regardless of what such an action is called. This includes, but is not limited to, suspension actions, settlement agreements and situations where an individual or entity voluntarily withdraws from the program or Health Plan provider network to avoid a formal sanction.

The Health Plan shall submit the written notification to both DHHS OIG and copy MPI via email. Document information examples include but are not limited to court records such as indictments, plea agreements, judgments, and conviction/sentencing documents.

Office of the Inspector General OIG:
sanction@oig.hhs.gov
Lieu of email use listed address below:
Attention: Florida Exclusions
Office of the Inspector General
Office of Investigations
Attention: Kathy Pettit
P.O. Box 23871
Washington D.C. 20026

With a copy of MPI at:
Attention: Florida Exclusion
Office of Inspector General
Medicaid Program Integrity
2727 Mahan Drive, M.S. #6
Tallahassee, FL 32308-5403

☒ **Freedom Health, Inc.** ☒ **Optimum HealthCare**	**Policy Title: Delegation Oversight** **Primary Department: Compliance** **Policy Number: COMP 09** ☒ **Medicare**
Approved By: _____ _____ Krista Gibbons *Manager Delegation Oversight* *Date* Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 01/01/2009** **Effective Date: 01/01/2009** **Revision Date(s): 6/4/2010; 7/31/2011; 2/29/2012; 4/5/2013; 1/15/2014; 04/27/2016; 12/01/2016, 04/27/2020**
Reference: CMS: 42 CFR Parts 422 and 423; Medicare Managed Care Manual Chapter 21; CMS Prescription Drug Benefit Manual Chapter 9; Medicare Managed Care Manual Chapter 11	

POLICY:

The Plan by written contract may delegate certain functions under its contracts with State and Federal Regulatory Agencies. Functions which may be delegated in whole or in part through the delegation process include: network development, credentialing, utilization management; quality improvement; member services, and claims processing/payment. Under a partial delegation, the Plan may retain certain responsibilities. The Plan shall oversee and remains accountable for any functions and responsibilities that it delegates. The Delegation Agreement does not relieve the Plan of its responsibility for the performance of duties through its contractual obligations with State and Federal Regulatory Agencies. In order to ensure that contracted entities that perform functions on behalf of Plan are in accordance with the terms of the Delegation Agreement, Accreditation Standards, and State and Federal Regulations, the Delegation Oversight Committee ensures the following:

- Written Agreements specify the delegated activities and reporting requirements
- Prior to any delegation, evaluates the Entity's ability to perform the delegated activities
- Conducts formal evaluation of the Entity's performance at least annually
- Implements remedies including corrective actions, revocation and/or termination if the Entity does not fulfill their obligations or performance is inadequate
- Conducts ongoing monitoring of entity's performance through report monitoring and focus audits
- Ensures audit findings are reported through the Delegation Oversight Committee

The Delegation Oversight Committee (DOC) is comprised of key leadership across the organization including but not limited to senior level executives and meets at least quarterly. The delegation and oversight activities are also reported to the Compliance and Quality Management Steering Committees

on at least a quarterly basis. These reports are then rolled up and presented at the Board of Directors level.

PROCEDURE:

Initial (Pre-Delegation) Process

1. The Business Owner will submit a pre-delegation request to the Delegation Oversight Area.

2. Delegation Oversight will schedule the pre-delegation audit. Pre-delegation audits and/or new site locations should be performed onsite and/or via desktop audit.

3. The designated auditor will conduct the pre-delegation audit and evaluate the Entity's ability to perform the delegated functions.

4. All findings are appropriately documented and routed to the attention of senior leadership including the business owner.

5. The auditor reports the pre-delegation audit findings to the Delegation Oversight Committee (DOC).

6. The DOC determines if delegation is to be recommended based on the findings from the pre-delegation assessment. The Entity is recommended for approval if:

    - The elements of the pre-delegation assessment are met, or
    - Any deficiencies identified are not egregious and will be remediated prior to delegation effective date

7. If approved for delegation, the Delegation Oversight Manager in partnership with the business owner will facilitate the execution of the Delegation Agreement for each appropriate Plan.

8. Appropriate regulatory agency notification prior to the effective date of the delegated activities is required as outlined below:

Medicare- Changes to First Tier/Downstream/Related Contracts (FDR) for Key Part C and Part D Functions require sixty (60) day notification to the CMS Account Manager prior to the effective date of the new contract.

On-going Entity Oversight Process

1. Delegation Oversight conducts ongoing quarterly monitoring of delegated activities.

2. Quarterly score cards are reviewed and analyzed by the delegation oversight auditors. If metrics are not meeting compliance, auditor communicates with entity to determine cause of non-compliance and actions for remediation.

3. If risk items are identified the plan may conduct adhoc focus or targeted audits.

Annual Audit Oversight Process

1. Delegated Entities are audited at least annually, and the auditor reports the findings to the Delegation Oversight Committee. If risk items are identified Plan may request documents or issue a corrective action plan.

2. Auditors that perform the Credentialing and Utilization Management audits will utilize the following NCQA file review audit methodology when conducting the annual oversight audit:
    - 5% or 50 files or 8/30 Audit Methodology

3. If the Entity is placed on a corrective action plan (CAP), the auditor is responsible for monitoring the CAP and reporting the CAP closure and successful validation of the remediation to the Delegation Oversight Committee.

4. The Delegation Oversight Committee determines if delegation is to be continued without interruption, continued under CAP, suspended, revoked or terminated based on the results of the audit and the CAP remediation.

Revocation of Delegation

Delegation may be revoked in instances where the Plan or a Governmental Authority determines that an Entity has not performed satisfactorily, including failing to implement a corrective action plan or quality improvement plan. The Plan can also terminate the Delegation Agreement at any time for cause related to egregious deficiencies.

☒ Freedom Health, Inc. ☒ Optimum HealthCare	**Policy Title: Conflict of Interest** **Primary Department: Compliance** **Policy Number: COMP 10** ☒ **Medicare**
Approved By: Diane E.A. Kortsch 06/05/2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 03/28/2012** | **Effective Date: 04/01/2012** **Revision Date(s): 04/01/2012 - Formerly COMP31; 05/01/2013; 04/01/2016; 06/05/2020**
Reference: Medicare Managed Care Manual Chapter 21; CMS Prescription Drug Benefit Manual Chapter 9	

POLICY:

Associates are required to perform their responsibilities in a manner that furthers the organization's interests, and that does not compromise those interests due to actual or perceived conflicts with other business or personal concerns. Associates are expected to exercise sound judgment and concern for the organization's interest to avoid situations that may cause actual harm or create the appearance of impropriety. A conflict of interest arises when associates' personal interests or activities influence, appear to influence, or may influence, their ability to act in the best interest of the organization.

Associates must refrain from any employment, activity, business or commercial interest or other affiliations, and relationships or interests that interfere with the associate's obligations to the organization. Associates must avoid situations that could adversely affect the exercise of good judgment in the performance of their duties; and abstain from circumstances where an associate and/or a third party may profit at the expense of or would otherwise have an adverse impact on the organization.

Purpose: The conflict of interest process exists to evaluate associates' activities or involvement with an individual or entity that could interfere with their responsibilities or might create the appearance of impropriety, and to provide guidance to associates for avoidance of situations that are in conflict with their responsibilities to the organization.

Key Principle: A conflict of interest is any activity or involvement with an individual or entity that adversely influences, or creates the appearance of adversely influencing, an associate's judgment, decisions, or actions in meeting the associate's responsibilities to the organization. Conflicts of interest may arise in many situations, including but not limited to, outside employment, board membership, investments, consulting or contractual relationships, and the acceptance of business courtesies, gifts or entertainment.

Conflicts of interest may arise based on an associate's or his/her family members' activities. The organization's work environment should be free of conflicts of interest that may interfere with an associate's responsibilities or may create the appearance of impropriety.

The organization's conflict of interest process helps the company comply with the Federal Sentencing Guidelines that state an "organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program."

Definitions: The following definitions apply for purposes of this policy.

Conflict of Interest: When an associate's personal interest or activities may influence or may appear to influence his/her judgment in the performance of his/her duties and obligations to the organization.

Family Members: An associate's spouse (wife or husband), children (daughter, son, step- daughter, step-son, daughter in-law, son in-law), siblings (sister, brother, step-sister, step-brother, sister in-law, brother in-law), parents (mother, father, step-mother, step-father, mother in-law, father in-law), domestic partner, fiancé, any person living with the associate, and any person close to the associate that may create an actual or perceived conflict of interest.

Affiliated Organization: Any corporation or organization of which an associate is a board member, an officer, a partner, manager or employee, or in which an associate is directly or indirectly a debt holder or the beneficial owner of any class of equity securities.

Financial Interest: If the person has, directly or indirectly, through business, investment, or immediate family member has ownership or potential investment in an entity with which the organization has or is negotiating a transaction or arrangement.

Public Companies: Those whose shares are traded on a stock exchange, such as the NYSE or Nasdaq, or in an over-the-counter market.

PROCEDURE:

Duty to Disclose:

1. Associates, as a condition of employment, will fully disclose any existing or potential conflicts of interest when hired and annually during annual training. Associates are also required to update the Conflict of Interest Form as a result of any change of status that may create a conflict of interest within 30 days of the change by sending an email to COI@freedomh.com, contacting the Compliance Department directly or by utilizing credentials to log into the Compliance System at https://compliancetraining.freedomh.com/Login/Login.aspx and accessing the Conflict of Interest module. Associates are required to disclose any potential or actual conflicts of interest to their manager and disclose the matter to the Compliance Department by completing the Conflict of Interest Form which can be found on the Compliance Page on the company intranet.

2. The Compliance Department oversees the Conflict of Interest Disclosure process, including the review of the Conflict of Interest disclosures. The Compliance Department will coordinate with Legal and Human Resources departments, and business unit leads as appropriate, to assess disclosures and to implement mitigation plans, as necessary. The Compliance Department

collects the disclosures of associates who have family members employed by the organization and provides periodic reports to Human Resources so they may review to ensure no prohibited relationships have been disclosed.

3. Compliance Department management may report Conflict of Interest disclosure results to the Board of Directors, President of Medicare Markets and any other members of management, as appropriate.

4. Human Resources, members of management and Legal may consult with the Compliance Department regarding Conflict of Interest mitigation plans.

5. All Associates will be informed and educated, under the auspices of the organization's Conflict of Interest Policy and Standards of Conduct, of their ongoing duty to disclose and update information related to potential Conflicts of Interest.

Associates may be subject to disciplinary action, up to and including termination of employment for failing to complete the Conflict of Interest Form or for failing to disclose an actual or perceived conflict of interest.

Examples of Conflicts of Interests:

Conflicts of interest may arise in many situations. Below are some of the common situations an associate may encounter. This is not intended to represent a comprehensive list of conflicts of interest. Even if a particular situation is not expressly mentioned herein, Associates are advised to disclose all potential conflicts, which may result in a violation of the conflict of interest policy.

1. Personal financial interest

   Associates may not own, directly or indirectly, a significant financial interest in any business that does business with, seeks to do business with, or competes with the organization. In general, a significant financial interest is ownership by an associate and/or an immediate family member of more than one percent of the outstanding securities/capital value of a business entity, or that represents more than five percent of the associate's total assets and/or those of an immediate family member.

   Associates must not refer customers, members, beneficiaries or those who do business with the organization to an entity in which the associate or a family member has a financial or other material interest. Some unique situations may qualify as an exception to this policy. The Compliance Department will address any exceptions on an individual basis. In addition, exceptions to this policy may require the Compliance Officer's written approval.

2. Outside employment

   Associates may not use company time, name, assets or the services of other associates for any outside activities unless authorized by company policies. An associate's primary employment obligation is to the organization and any external activities, such as a second job or a personal

business, must not conflict with the associate's obligations. Associates must notify their manager and disclose the matter on the Conflict of Interest Form. The associate's manager and the Compliance Department will help the associate determine if the outside employment or other external activities presents a conflict. In many situations, the Compliance Department can work with managers and associates to develop mitigation plans to help prevent any actual or perceived conflicts. Associates may be required to disassociate from the conflicting relationship as a condition of continued employment.

3. Service on an external board of directors

   Any associate who wishes to serve on any board of directors must disclose this information on the Conflict of Interest Form prior to accepting the board appointment and provide relevant information to the Compliance Department.

   Public Company Board: Associates who wish to serve on the board of a Public Company must contact the Compliance Department prior to accepting the board appointment. The Compliance Department will gather information from the associate and the associate's manager to determine if any conflict exists. Public Company Board assignments also require pre-approval by the Compliance Officer, Legal and the President of Medicare Markets. Compliance facilitates this approval process and notifies the associate of the outcome.

   Non-profit or Private Boards: Associates who wish to serve on the board of a non-profit organization or a privately owned company must contact the Compliance Department prior to accepting the board appointment. The Compliance Department will gather information from the associate and the associate's manager to determine if any conflict exists. If the associate will receive compensation (cash, equity) to serve on these types of boards, the board appointment requires the pre-approval of the Compliance Officer and the applicable senior management members. Compliance facilitates this approval process and notifies the associate of the outcome.

4. If an associate is serving on the board of a private company, and the company then later becomes a Public Company, the associate must notify the Compliance Department as soon as possible. The Compliance Department will obtain information for review by management.

5. Family and personal relationships

   Employment of relatives and individuals involved in personal relationships with associates is allowed as long as those individuals are the best qualified candidates for the job, and it is not a prohibited relationship.

   A prohibited relationship occurs if the hiring, promoting or transferring of an associate's family member or someone with whom the associate has a personal relationship would result in the creation of a supervisory/subordinate relationship, or the appearance of any other potential or actual conflict of interest.

   The associate cannot make decisions involving the hiring, promoting, transferring, compensation, performance evaluation, corrective action or termination of a family member's

employment, or any others with whom the associate has a personal relationship with (including temporary workers, contractors, vendors, etc.)

6. Someone close to you working in the industry

   Associates may find themselves in a situation where a spouse, family member or others close to the associate has a relationship with a competitor or another business in the Health Care industry. These situations require extra sensitivity and need to be disclosed on the Conflict of Interest Form which will be reviewed by the Compliance Department.

Violations:

Violations of this Conflict of Interest Policy are to be brought immediately to the attention of the Compliance Officer or Human Resources to ensure appropriate investigation and remedial action.

Record Retention: The Conflict of Interest Forms completed in the Compliance System, and all other supporting documentation utilized in the approval, denial and disclosure process including mitigation plans will be maintained for a period of 10 years.

Attachment A
Conflict of Interest Questionnaire

To be fully completed by directors; officers; employees; and contractors (collectively "Associates).

Please use additional sheets if it is necessary to supplement your answers. If the answer to each question below is "None", please state so.

Name of Associate: _____ Title: _____ Date_____

1. Do you have any Immediate Family Members who are employed with the organization?

Immediate Family Member Means: your spouse, parent, stepparent, child, stepchild, siblings, mother-in-law, father-in-law, son-in-law, daughter-in-law, brother-in-law, sister-in-law and anyone (other than a tenant or domestic associate) who shares such associate's home.

Name of immediate Family Member	Job Title of Immediate Family Member

2. Do you and/or any of your immediate Family Members own either individually or collectively, any equity or voting interest, have control of, a significant influence or ownership in any entities that do business with the organization?

Control means: possession, directly or indirectly, of the power to direct or influence the direction of the management and policies, whether through ownership, voting securities, by contract or otherwise.

Relationship means: any employment (wages, salaries, fees, etc.), financial interest, consulting, contractual agreements/arrangement, Board of Directors, entities that either you or your family member have control of, significant influence over, or are a principal owner, or any other affiliation or interest of any kind.

Name of individual and relationship to you	Name of the organization you/immediate family member have control or ownership in	Percentage of Ownership	Nature of Business

3. List any other relationships not previously disclosed in the prior questions with any: Providers of Health Care Services, Alternate Care Delivery Systems, Suppliers of Health Care Needs, Medical Billing Entities, Health Insurance Companies or Related Organizations, Health and/or Life Related Insurance Agents, Brokers, or Other Insurance Affiliates, Medicare or Medicaid Contractors, Local/State/Federal Government Agencies with Health Care responsibilities, Health Care Professional or Trade Organizations, or Suppliers of Goods and/or Services to the Company.

Type of Relationship: Executive, Non-Management, Ownership, Contractual, Consulting, Board Member, Other

Name of Organization	Type of Organization	Individual who has the relationship with the Organization	Type of Relationship-

4. List the individual and the organization that you have accepted/received any gifts, special courtesies, payments or entertainment such as sporting event tickets, dinners, golf, spas, etc. (other than common business courtesies such as pens or coffee mugs which are reasonable in nature and amount) doing or seeking to do business with the organization under a government contract.

Name of Individual you received the gift, special courtesy or payment from	Name of the Organization individual represents	Description of Gift, Courtesy or Payment	Reason for Gift	Estimated Retail Value

5. List any employment outside the organization or any business you or an immediate family member own that does business with, seeks to do business with, or competes with the organization.

Name of Organization you are employed with or have ownership	Your Job Title	Role or Responsibilities

6. List any participation on non-profit/charitable or for-profit organizations' Boards of Directors, Advisory Groups, Industry Associations, compensated medical or pharmaceutical research/studies, etc.

Name of Board, Advisory Group, Industry Association	Date of Appointment/Engagement	How Compensated- Receive Equity or Stock

7. List any participation on a Board of Directors or similar governing body as part of your job responsibilities for any organization owned investments or joint ventures.

A board position means a board of directors (or similar governing body) role such as a chair, director, manager, etc. for an entity where the organization has a partial ownership, minority ownership interests, or a joint venture.

Name of Entity	Your Job Title	Role or Responsibilities

Conflict of Interest Policy Attestation

I have received and read the Company's Conflict of Interest Policy. I understand the policy, my duties and responsibilities to comply with its provisions, and the consequences of non-compliance. I certify that I am in compliance with the policy, know of no violation of or deviations from the policy, have raised all issues concerning actual or potential conflicts of interest in writing with the Human Resources Director, the Compliance Officer or Corporate Counsel, as appropriate, and that my responses to the above questions are complete and correct to the best of my knowledge. I agree that if I become aware of any information that might indicate that this disclosure is inaccurate or that I have not complied with this Conflict of Interest Policy, I will notify the appropriate Company representative.

_____

Associate Name and Title

_____

Signature

_____

Date

☒ Freedom Health, Inc. ☒ Optimum HealthCare	**Policy Title: HIPAA Privacy and Breach Notification** **Primary Department: Compliance** **Policy Number: COMP 11** ☒ **Medicare**
Approved By: Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 03/28/2012** **Effective Date: 04/01/2012** **Revision Date(s):** **04/01/2012 formerly COMP30 & COMP17; 06/1/2012, 08/15/2013, 05/06/2016; 04/27/2020**
Reference: American Recovery and Reinvestment Act of 2009 ("ARRA"), Health Information Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH"), 45CFR Parts 160 and 164;	

POLICY:

The Health Plan governs the use and disclosure of Protected Health Information ("PHI"), as well as what steps are taken in the event unsecured PHI is breached in a manner prohibited under HIPAA. The Health Plan reserves the right to amend or change these Policies and Procedures at any time in, compliance with ARRA, HIPAA, and HITECH requirements.

Security Rule

It is the policy of the Health Plan to fully comply with the HIPAA Security Rule, including to:

1. Ensure the confidentiality, integrity, and availability of all electronic PHI ("ePHI") that the Health Plan and/or business associates create, receive, maintain, or transmit;
2. Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI;
3. Identify and protect against reasonably anticipated uses or impermissible disclosures of ePHI that are not permitted or required under HIPAA; and
4. Ensure compliance with the HIPAA Security Rule by all associates.

The VP of Information Systems has been designated as the Security Officer and is responsible for the development and implementation of security policies and procedures. The Security Officer and Privacy Officer may coordinate privacy and security efforts.

Privacy Rule

It is the policy of the Health Plan to fully comply with the HIPAA privacy rule. The organization's Compliance Officer acts as the Privacy Officer and is responsible for:

1. The development and implementation of privacy policies and procedures that are consistent with the Privacy Rule.
2. Ensuring workforce members, including CEO, senior administrators, managers, governing body members, and FDRs are trained on its privacy policies and procedures.
3. Providing individuals with information on the Health Plan's privacy practices.
4. Coordinating the investigation of privacy complaints.
5. Coordinating the mitigation of any privacy violation.
6. Handling of breach notification(s).

Additionally, the purpose of this policy is to set forth the Health Plan's process for the use and disclosure of the Protected Health Information (PHI) for prospective, current, and former member(s). It is the policy of the Plan to disclose PHI, for purposes other than treatment, payment, or health operations, only pursuant to a valid, written authorization, unless such use or disclosure is otherwise permitted or required by law. Use or disclosure pursuant to an authorization will be consistent with the terms of such authorization. The Privacy Rule protects all "individually identifiable health information" created, received, maintained, or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

PROCEDURE:

Training

The Health Plan has implemented effective HIPAA training and education for its employees, including CEO, senior administrators, managers, and its governing body members. The training and education is made a part of the orientation for new employees and occurs annually thereafter as a condition of employment. Training is developed in accordance with Regulatory guidance and other pertinent Federal and state laws. Content is reviewed at least annually for updates and revisions and approved for use by the Privacy Officer and Senior Management. Additionally, the Compliance Trainer or designee provides oversight of the training through electronic monitoring and tracking. The Health Plan maintains a separate policy and procedure for Training.

Use and Disclosure of PHI

The Health Plan has implemented policies and procedures for granting, documenting, reviewing, and modifying a user's right of access to a workstation, transaction, program, or process. All employees are authorized to access PHI to the extent performance of their job functions reasonably requires such access and where access is necessary in furtherance of legitimate, HIPAA-approved purposes of payment, treatment and health care operations. Employees may not access PHI except in accordance with the Plan's HIPAA policies and procedures and only in furtherance of proper business-related activities. The Plan maintains separate policies and procedures for Physical and Technical Safeguards.

The Health Plan's employees must ensure that requested PHI is not used for non-health related purposes, unless otherwise permitted or required by law. In general, PHI cannot be given to an employer, used or shared for marketing or various other purposes unless the member has provided

signed permission/authorization specifying who will get the information and what it will be used for. The individual's written authorization is required for any use or disclosure of PHI that is not for treatment, payment, healthcare operations or otherwise permitted or required by the Privacy Rule.

Valid Authorizations

In addition to the authorization having to be written in "plain language", there are certain elements it must contain according to the HIPAA Privacy Rule in order for it to be considered valid. If any one element is missing, the Privacy Rule prohibits the disclosure of the information.

All of the following elements must be included in an authorization:

1. A specific and meaningful description of the information to be disclosed.
2. The name or other specific identification of the person (or organization or class of persons) authorized to make the requested disclosure.
3. The name or other specific identification of the person (or organization or class of persons) to whom the information will be disclosed.
4. The purpose of the requested disclosure. (If the member initiates the authorization, the statement "at the request of the member" is a sufficient description of the purpose).
5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.
6. Signature of the individual and date. If the authorization is signed by a personal representative, a description of such representative's authority to act on behalf of the member must also be provided.

In addition to the core elements, above, the authorization must contain statements regarding the following:

1. The individual understands they have the right to revoke the authorization in writing except to the extent that action has already been taken based on the authorization.
2. The individual understands that signing the authorization is voluntary and their treatment, payment, enrollment in the Health Plan, or eligibility benefits will not be conditioned upon the individual's authorization of disclosure.
3. The individual understands that information disclosed under the authorization may be subject to redisclosure by the recipient, and may no longer be protected by federal or state law.
4. If the Health Plan seeks an authorization for use and disclosure of PHI, the Health Plan must provide a copy of the signed authorization to the individual.

The Health Plan makes all reasonable efforts to limit the use and disclosure of PHI. Employees abide by the HIPAA "Minimum Necessary" standard (i.e., that amount and type of PHI requested, accessed, used and/or disclosed shall be limited to information that is needed to accomplish the intended, authorized purpose of the use, disclosure, or request). Use and disclosure to other

authorized employees, plan administrators, authorized representatives, brokers and/or other business associates will be made in accordance with the Minimum Necessary Standard.

The Health Plan may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the Health Plan obtains satisfactory assurance that the business associate will appropriately safeguard the information. A business associate may use or disclose PHI as permitted by their business associate agreement or as required by law.

Minimum Necessary does not apply to:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual, as permitted or as required by HIPAA;
- Uses or disclosures made pursuant to an authorization;
- Disclosures made to the Secretary in accordance with HIPAA;
- Uses or disclosures that are required by law; and
- Uses or disclosures that are required for compliance with applicable requirements.

The following procedures are followed in situations of permitted uses and disclosures:

1. Verification of the identity of the individual requesting PHI – Reasonable steps must be taken to verify the identity and authority of all persons requesting access to PHI before making any disclosure. If the identity or authority of the person making the request is at all in question, employees are directed to contact the Privacy Officer. At a minimum, associates are expected to verify the following elements:
    a. Member Name
    b. Member Address
    c. Member Phone Number
    d. Member Date of Birth

2. Use and Disclosure to Parent or Legal Guardian of Minor Child – Employees may disclose PHI to the parent or legal guardian of a minor child, so long as appropriate steps are taken to verify the identity of the person making the request and to confirm relationship between the person and the minor child.

3. Use and Disclosure to Third Parties – Employees may not disclose PHI in response to a request from a third-party claiming to have authorization from the member unless sufficient written authorization has been verified and the disclosure has been approved by the Privacy Officer.
    a. Personal (Authorized) Representative: If a PHI disclosure request is made by a member's personal representative, employees will use internal system(s) to verify the authorized representative. If the associate is unable to validate, documentation will be requested to confirm the individual's authority. Upon receipt, the documentation will be reviewed by the Privacy Officer, Legal or their designee.

b. Use and Disclosure to Spouse(s), Family Member(s), or Friend(s): Employees are not permitted to disclose PHI to spouses, family members or friends of members, absent express written authorization from the member. All request for the disclosure of PHI received from a spouse, family member or friend (excluding requests from the parent or legal guardian of a minor child) must be referred to the Privacy Officer, Legal, or their designee, in order to ensure that the proper authorization has been obtained before making the disclosure.

c. Use and Disclosures with the member present: Employees may use or disclose to a family member, other relative, or a close personal friend of the member, or any other person identified by the individual, protected health information directly relevant to the members' care or payment related to the individual's health care, if the employee has

   - Obtained the member's agreement/consent; or
   - Provides the member with the opportunity to object to the disclosure, and the member does not express an objection

d. Deceased Persons: A copy of the certified death certificate must accompany the documentation indicating the individual requesting the information acts as executor of the will.

e. Partially De-Identified Information: We may use and disclose "partially de-identified" health information for public health and research purposes, or for business operations, if the person who will receive the information signs a business associate agreement to protect the privacy of the information as required by federal and state law. Partially de-identified health information will not contain any information that would directly identify the individual (i.e. name, address, social security number, phone number, etc.)

f. Use and Disclosures for research: We may use PHI to perform select research activities, provided that certain established measures to protect the individual's privacy are in place.

g. Disaster Relief Purposes: We may disclose PHI to a public or private entity authorized by law to assist in disaster relief efforts.

4. Disclosures to HHS, Law Enforcement or Other Administrative or Judicial Authorities – Employees must not disclose PHI in response to requests by HHS, law enforcement agents or other government or administrative authorities. Any and all such requests (including subpoenas, court orders, discovery requests, public health, criminal or civil investigations, etc.) are referred to the Privacy Officer and/or Legal.

Potential Breach

All employees are expected to be vigilant with respect to guarding PHI, and will access, use and disclose PHI only as permitted under HIPAA. In the event that a potential breach of PHI occurs, the following procedures must be followed.

1. *Discovery* - A breach of PHI is deemed "discovered" as of the first day the Health Plan knows of the breach or, by exercising reasonable diligence, would or should have known about the breach. If a potential breach is discovered, it is very time sensitive and must be reported immediately.

   Breach Excludes:

   a. Any unintentional acquisition, access, or use of protected health information by an associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted.

   b. Any inadvertent disclosure by a person who is authorized to access protected health information at the covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the Health Plan participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted.

   c. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

   An acquisition, access, use or disclosure of PHI in a manner not permitted by law is presumed to be a breach unless the Health Plan or business associate demonstrates there is a low probability that the PHI has been compromised based on a risk assessment of the following factors:

   a. The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;

   b. The un-authorized person who used the PHI or to whom the disclosure was made;

   c. Whether the PHI was actually acquired or viewed; and

   d. The extent to which the risk to the PHI has been mitigated.

2. *Reporting*

   a. The Health Plan has implemented procedures and a system for promptly responding to a potential breach. Employees and/or business associates are educated on the mechanisms available for reporting a potential breach.

   b. The Health Plan does not tolerate retaliation or retribution against any associate, member, or FDR who makes good-faith reports of potential or suspected violations. The individual(s) may remain anonymous, if they choose. All information received is considered confidential and protected from retaliation.

c. Associates that believe a potential breach of PHI has occurred must immediately notify the Privacy Officer. Reporting mechanisms have been established by the Privacy Area and are available 24 hours a day, 7 days a week. These mechanisms are covered in training and posted in all employee workstations.

d. The associate is encouraged to provide all of the information available regarding the potential breach, including names, dates, the nature of the PHI potentially breached, the manner of the disclosure (fax, email, mail, verbal), names of employees involved, the recipient, all other persons with knowledge, and any associated written or electronic documentation that may exist.

e. Notification and associated documentation may itself contain PHI and should only be given to the Privacy Officer.

f. Associates are instructed not to discuss the potential breach with anyone else, and must not attempt to conduct an investigation.

3. *Investigation* - Upon receipt of notification of a potential breach the Privacy Officer, or his/her designee, promptly conducts an investigation.

   a. Research efforts include, but are not limited to, the collection of facts, review of regulatory guidance, contact with members and/or providers, request(s) for information from the organization's departments, and interviews with appropriate associates.

   b. All research, inquiries, and other investigative activities are kept within the smallest number of individuals in order to ensure confidentiality whenever feasible.

   c. Information obtained during an investigation is documented and included in the case file. Information obtained may include supporting documentation, such as: recorded interviews, written responses, copy of letters/claims, etc.

   d. Actions taken, and factual information assembled, are documented in the case notes.

4. *Risk Assessment and Recommendation* - Upon completing the investigation, the Privacy Officer performs and appropriately documents a Risk Assessment. The purpose of the Risk Assessment is to determine if a use or disclosure of PHI constitutes a breach.

   A "reasoned judgment" standard is applied to the Risk Assessment, which is fact specific, and considers the following factors:

   - Did the disclosure involve Unsecured PHI in the first place?
   - Who impermissibly used or disclosed the Unsecured PHI?
   - To whom was the information impermissibly disclosed?
   - Was it returned before it could have been accessed for an improper purpose?
   - What type of Unsecured PHI is involved and in what quantity?
   - Was the disclosure made for any improper purpose?

- Is there the potential for significant risk of financial, reputational, or other harm to the individual whose PHI was disclosed?
- Was immediate action taken to mitigate any potential harm?
- Do any of the specific breach exceptions apply?

5. *Final Determination by the Privacy Officer* - The Privacy Officer has final authority to determine whether a breach of PHI occurred and what, if any, further action is warranted.

   In the case of a breach which has been clearly demonstrated to be founded and supported by evidence, a corrective action is issued by the Privacy Officer.

   a. The corrective action is designed to correct the underlying problem that resulted in program violations and to prevent future breach.

   b. The corrective action may provide timeframes for specific achievements towards addressing the deficiency. Follow-up on all corrective actions are done by the Privacy Officer or designee to ensure that the risk has been properly addressed.

   c. If corrective actions are not properly implemented or corrected appropriately, disciplinary measures are taken including and up to termination of the associate or contract.

6. *Notification To Individuals* – Following the discovery of a breach of unsecured protected health information, the Health Plan will notify each individual whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach. The Health Plan provides notification without reasonable delay and in no case later than 60 calendar days after the discovery of the breach.

   a. The notification shall be written in plain language and must include, to the extent possible:

      - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
      - A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, diagnosis, or other types of information were involved).
      - Any steps individuals should take to protect themselves from potential harm resulting from the breach;
      - A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
      - Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

b. The notification will be provided in the following form:

- *Written notice:* Written notification will be sent by first-class mail to the individual at the last known address of the individual, or if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. If the individual is deceased, the notification will be sent by first-class mail to the next of kin or personal representative of the individual, if known.

    i. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual will be provided. If the individual is deceased, substitute notice need not be provided in the case in which there is insufficient or out-of-date contact that precludes written notification to the next of kin or personal representative of the individual.

    ii. In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

    iii. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice must:

        - Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
        - Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.
        - In any case deemed by the Health Plan to require urgency because of possible imminent misuse of unsecured PHI, The Health Plan may provide information to individuals by telephone or other means as appropriate.

7. *Notification to the Media*- For a breach of unsecured protected health information involving more than 500 individuals, the Health Plan is required, following the discovery of the breach, to notify the affected individuals and prominent media outlets serving the State or jurisdiction. The Health Plan provides notification without reasonable delay and in no case later than 60 calendar days after the discovery of the breach.

8. *Notification to the HHS Secretary* – Following the discovery of a breach of unsecured protected health information, the Plan notifies the Secretary.
    a. For breaches of unsecured protected health information involving 500 or more individuals, the Health Plan shall provide the notification contemporaneously with the notification to the individual and in the manner specified on the HHS Web site.
    b. For breaches of unsecured protected health information involving less than 500 individuals, the Health Plan maintains a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provides the notification required for breaches discovered during the preceding calendar year, in the manner specified on the HHS Web site.

9. *Notification by a Business Associate* – A business associate is required, following the discovery of a breach of unsecured protected health information, to notify the Health Plan of such breach.
    a. A business associate must provide the Health Plan with the required notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
    b. The notification must include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.
    c. A business associate is expected to provide the Health Plan with any other available information that the Health Plan is required to include in the notification to the individual, at the time of the notification or promptly thereafter as information becomes available.

10. *Law Enforcement Delay* - A delay in notification is permissible if a law enforcement official states that a breach notification would impede a criminal investigation or cause damage to national security.
    a. In that event, the law enforcement statement must be in writing and must specify the length of the delay required.
    b. If the request for a delay in notification is oral, the Plan must document the statement, including the identity of the official and request written confirmation within 30 days. If no written request for a delay is received within that time, the Plan must send notification of the breach.

All HIPAA investigations, including their dispositions are reported to Senior Management, Compliance Committee and Board of Directors on a quarterly basis.

Member Rights

The Health Plan educates employees and business associates on the importance of member's rights, including:

1. *Notice of Privacy Practices* - An individual's right to adequate notice of the uses and disclosures of protected health information that may be made by the Health Plan or business associates and of the individual's rights and the Health Plan's legal duties with respect to protected health information.

   This notice is provided to members at the time of enrollment, to individuals currently covered by the Plan annually and within 60 days of a material revision to the notice. The Plan provides the revised notice and/or information on how to obtain a copy of the notice. Additionally, the notice is made available on the Health Plan's website and/or upon request. No less frequently than once every three years the Plan notifies individuals covered by the Plan of the availability of the notice and instructions on how to obtain the notice.

   The Notice must be written in plain language and contain the following elements as set forth by HIPAA:

   a. *Header:* The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

   b. *Use and disclosures*- The notice contains:

      - A description, including at least one example, of the types of uses and disclosures that the Health Plan is permitted to make for each of the following purposes: treatment, payment, and health care operations.
      - A description of each of the other purposes for which the covered entity is permitted or required to use or disclose protected health information without the member's written authorization.
      - If a use or disclosure for any purpose described above is prohibited or materially limited by other applicable law, the description of such use or disclosure will reflect the more stringent law.
      - For each of the above, the description includes sufficient detail to place the member on notice of the uses and disclosures that are permitted or required.
      - A statement that other uses and disclosures will be made only with the member's written authorization and that the member may revoke such authorization.

   c. *Individual rights:* The notice contains a statement of the individual's rights with respect to protected health information and a brief description of how the member may exercise these rights, as follows:

      - The right to request restrictions on certain uses and disclosures of protected health information, including a statement that the covered entity is not required to agree to a requested restriction;

- The right to receive confidential communications of protected health information
- The right to inspect and copy protected health information
- The right to amend protected health information
- The right to receive an accounting of disclosures of protected health information
- The right to receive a paper copy of the noticed upon request, when the member has agreed to receive the notice electronically

d. *Health Plan's duties*- The notice includes:

- A statement that the Health Plan is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured PHI;
    - A statement that the Health Plan is required to abide by the terms of the notice currently in effect; and
    - A statement that the Health Plan reserves the right to change the terms of its notice and to make new notice provisions effective for all protected health information that it maintains. The statement will also describe how it will provide members with a revised notice.

e. *Complaints* - The notice contains a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the Health Plan, and a statement that the member will not be retaliated against for filing a complaint.

f. *Contact* - The notice contains the name, title, and telephone number of a person or office to contact for further information.

g. *Effective date* - The notice contains the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

2. *Confidential Communication* - An individual has a right to receive confidential communications of PHI.

a. Requests for confidential communication must be submitted in writing. Although members are not required to complete an Authorization Form, one will be made available to individuals via the Plan's website and/or upon request.

b. The Health Plan will accommodate reasonable requests by individuals to receive communications of protected health information by alternative means or at alternative locations, if the member clearly states that the disclosure of all or part of that information could endanger the member.

c. The Health Plan does not require an explanation from the member as to the basis for the request as a condition of providing communications on a confidential basis.

3. *Access to PHI* - Except for Psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding HIPAA requires that members be afforded the opportunity to access certain PHI within a Designated Record Set. The Designated Record Set includes enrollment, payment, and claims adjudication records, and other PHI used by or for the Plan to make coverage decisions about an individual.

    a. Depending on the type of PHI, members may submit request for access to PHI by phone, fax, email, or mail.

    b. Requests will be reviewed and acted upon no later than 30 days after receipt of the request. If the Health Plan is unable to take an action within the time required, the Health Plan may extend the time for such actions by no more than 30 days, provided that the Health Plan provides the individual with a written statement of the reasons for the delay and the date by which the Health Plan will complete its action on the request.

    c. If the Health Plan does not maintain the PHI that is the subject of the individual's request for access, and the Plan knows where the requested information is maintained, the Health Plan will inform the individual where to direct the request for access.

    d. The Health Plan will deny a request for access without providing the member an opportunity for review if the PHI is excluded from the right of access:

        - Psychotherapy notes;
        - Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

    e. The Health Plan may deny a member access to PHI:

        - If a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
        - If the PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that access requested is reasonably likely to cause substantial harm to such other person; or
        - The request for access is made by the individual's personal representative and a licensed health care profession has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person

    f. If access is denied on a ground permitted by HIPAA, in whole or in part, the Health Plan will provide the member with a written denial.

- The denial will be provided in plain language and contain:
    i. The basis for the denial;
    ii. A statement of the individual's review rights, including how the individual may exercise such review rights;
        - The member will be given an opportunity to have the denial reviewed by a licensed health care professional who is designated by the Health Plan to act as a reviewing official and who did not participate in the original decision to deny.
        - If the individual requests a review of a denial, the designated reviewing official will determine, within a reasonable period of time, whether or not to deny the access requested.
        - Upon determination, the Health Plan will promptly provide a written notice to the individual of the determination of the designated reviewing official and take other action as required to carry out the designated reviewing official's determination.
    i. A description of how the individual may complain to the Health Plan or to the Secretary. The description includes the Privacy Officer's name and telephone number.
- The Health Plan will, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI as to which the Health Plan has a ground to deny access.

g. If access is granted, in whole or in part, the Health Plan will inform the individual of the acceptance of the request in writing. The Health Plan will arrange a convenient time and place for the individual to inspect or obtain a copy of the PHI, or mail the copy of the PHI at the individual's request.
    - If the individual's request for access directs the Health Plan to transmit the copy of PHI directly to another person designated by the individual, the Health Plan will provide a copy to that individual. The request must be made in writing, signed, identify the designated individual and where to send the copy of PHI.
    - The Health Plan will provide access to the PHI in the form or format requested, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agree to by the Health Plan and the individual.
    - The Plan may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if:

ii. The individual agrees in advance to such a summary or explanation; and

iii. The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

4. *Amendments or corrections to PHI* - HIPAA requires members to be afforded the opportunity to have the Health Plan amend PHI or a record about the member that is maintained in the designated record set. The Designated Record Set includes enrollment, payment, and claims adjudication records, and other PHI used by or for the Plan to make coverage decisions about an individual.

   a. The Plan may require individuals to submit requests for amendments or corrections to PHI in writing. Although members are not required to complete an Authorization Form, one will be made available to individuals via the Plan's website and/or upon request.

   b. The request for amendment or correction must provide a reason to support the requested amendment.

   c. These requests are reviewed and acted upon within 60 days after receipt of such a request.

   d. If the Health Plan is unable to act on the amendment within the time required, it may extend the time for such actions by no more than 30 days, provided that:

      - The Health Plan, within the time limit set, provide the individual with a written statement of the reasons for the delay and the date by which the Plan will complete its action on the request; and
      - The Health Plan may have only one such extension of time for action on a request for an amendment.

   e. If the requested amendment is granted, in whole or in part, the Health Plan will take the actions within the timeframe specified above.

      - The Plan will make the appropriate amendment to the protected PHI or record that is the subject of the request for amendment by, at minimum, identifying the records in the designated records set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
      - The Plan will inform the individual that the amendment is accepted and obtain the individual's identification of an agreement to have the Plan notify the relevant person with which the amendment needs to be shared.
      - The Plan will attempt to inform the persons identified by the individual as having received PHI about the individual and needing the amendment and persons, including business associates, that the covered entity knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual, in writing within a reasonable time.

f. The Health Plan may deny an individual's request for amendment, if it determines that the PHI or record that is the subject of the request:

- Was not created by the Health Plan, unless the individual provides a reasonable basis to believe that the originator or PHI is no longer available to act on the requested amendment;
- Is not part of the designated record set;
- Would not be available for inspection (excepted); or
- Is accurate and complete.

g. If the requested amendment is denied on a ground permitted by HIPAA, in whole or in part, the Health Plan will provide the member with a written denial.

- The denial is provided in plain language and contains:
    i. The basis for the denial
    ii. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
        - The member will be given an opportunity to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement.
        - The Health Plan may prepare a written rebuttal to the individual's statement of disagreement. Whenever a rebuttal is prepared, the Plan will provide the individual who submitted the statement of disagreement with a copy of the rebuttal.
        - A statement that, if the individual does not submit a statement of disagreement, the individual may request that the Plan provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and
        - A description of how the individual may complain to the Plan or to the Secretary. The description includes the Privacy Officer's name, title, and telephone number.
- The Health Plan will identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the Plan's denial of the request, the individual's statement of disagreement, if any, and the Plan's rebuttal, if any, to the record set.
    i. If a statement of disagreement has been submitted by the individual, the Plan will include the material appended, or at the election of the Plan an accurate summary of any such

information, with a subsequent disclosure of the PHI to which the disagreement relates.

ii. If the individual has not submitted a written statement of disagreement, the Plan will include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action.

iii. When a subsequent disclosure is made using a standards transaction that does not permit the additional material to be included with the disclosure, the Plan will separately transmit the material to the recipient of the standard transaction.

- If the Plan is informed by another covered entity of an amendment to an individual's PHI, the Plan will amend the PHI in designated record sets as required by HIPAA.

5. *Accounting of Disclosures* - An individual has a right to receive an accounting of disclosures of PHI made by the Plan or business associate in the six (6) years prior to the date on which the accounting is requested, except for:

   - Disclosures the individual has authorized.
   - Disclosures made earlier than six years before the date of the request
   - Disclosures made for treatment, payment, and health care operations purposes except when required by law.
   - Certain other disclosures that are excluded by law.

   a. The accounting will include:

      - the date of each disclosure;
      - the name of the entity or person who received the PHI and, if known, the address of such entity or person;
      - a brief description of the PHI disclosed; and
      - a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of the written request for disclosure.

   b. Requests for accounting of disclosures are reviewed and acted upon within 60 days after receipt of such a request.

      - If the Health Plan is unable to provide the accounting within the time required, it may extend the time for such actions by no more than 30 days, provided that:

        i. The Health Plan, within the time limit set, provide the individual with a written statement of the reasons for the delay and the date by which the Plan will provide the accounting; and

ii. The Health Plan may have only one such extension of time for action on a request for an accounting.

c. The Health Plan will document and maintain the following:
   - The information required to be included in an accounting for disclosures of PHI that are subject to an accounting;
   - The written accounting that is provided to the individual;

d. The Plan may temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency provides the Plan with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such suspension is required.
   - If the agency or official statement is made orally, the Plan will:
   - Document the statement, including the identity of the agency or official making the statement;
   - Temporarily suspend the individual's right to the accounting of disclosures subject to the statement; and
   - Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

e. The member has the right to file a complaint with the Health Plan or the US government (www.hhs.gov/ocr/hipaa/) if they believe their rights are being denied or their health information is not being protected.

6. *Request Restrictions* - An individual has a right to request restrictions on certain uses and disclosures of PHI.

   a. Requests for restrictions to PHI must be submitted in writing. Although members are not required to complete an Authorization Form, one will be made available to individuals via the Plan's website and/or upon request.

   b. Requests to restrict the use and disclosures are reviewed and acted upon receipt of such a request.

   c. If the Plan agrees to a restriction, it will not use or disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment, the Plan may use the restricted PHI, or may disclose such information to a health care provider, to provide such treatment to the individual.
      - If restricted PHI is disclosed to a health care provider for emergency treatment, the Plan will request that the health care provider not further use or disclose the information.
      - A restriction agreed to by the Plan is not effective to prevent uses or disclosures permitted or required by HIPAA.

d. If the requested restriction is denied on a ground permitted by HIPAA, in whole or in part, the Health Plan will provide the member with a written denial.

e. The Health Plan may terminate its agreement to a restriction, if:

- The individual agrees to or requests the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented; or
- The Plan informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has so informed the individual.

Fees

The Health Plan may impose a reasonable, cost-based fee; notification of the Plan's policy regarding fees will be documented on the Privacy Notice.

1. Fees assessed for Access to PHI
    a. Labor for copying the PHI requested by the individual, whether in paper or electronic form;
    b. Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
    c. Postage when the individual has requested the copy, or the summary or explanation be mailed; and
    d. Preparing an explanation or summary of the PHI
2. Fees assessed for Accounting of Disclosures
    a. The Plan provides the first accounting to an individual in any 12 month period without charge.
    b. The Plan may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period provided the Plan has informed the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

Complaints

Individuals may file a file a complaint with the Health Plan if they believe their privacy rights have been violated.

To file a complaint, the individual may submit his/her concerns to the Privacy Officer using any of the mechanisms available, including the organization's hotline, fax, email or web portal (www.americas1stchoice.ethicspoint.com).

The Health Plan does not tolerate retaliation or retribution against any associate, member, or FDR who makes good-faith reports of potential or suspected violations. Individuals may remain

anonymous if they choose. All information received is considered confidential and protected from retaliation.

Individual may also file a complaint with the US government (www.hhs.gov/ocr/hipaa/).

Sanctions

The Privacy Officer or designee investigates suspected violations. Each action is considered on a case-by-case basis and disciplinary actions are imposed on a fair and equitable basis and consistently applied. Appropriate sanctions are instituted against employees and/or business associates who fail to comply with the Health Plan's HIPAA Privacy and Breach Notification Policies and Procedures contained herein.

The Health Plan maintains a separate policy and procedure for Disciplinary Actions.
Civil Penalties for HIPAA Privacy Rule Violations: The Department of Health and Human Services, Office for Civil Rights (OCR) is responsible for administering and enforcing the Privacy Rule and may conduct complaint investigations and compliance reviews. The Health Plan may be subject to civil monetary penalties of $100 to $50,000 or more per violation up to an annual cap of $1,500,000. A to civil monetary penalty will not be imposed for violations in certain circumstances, such as if:

1. the failure to comply was not due to willful neglect, and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of OCR); or
2. the Department of Justice has imposed a criminal penalty for the failure to comply.

Criminal Penalties for HIPAA Privacy Rule Violations: A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one-year imprisonment. The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm. The Department of Justice is responsible for criminal prosecutions under the Privacy Rule.

Record Retention and Documentation

The Health Plan will maintain copies of policies and procedures, established for compliance with HIPAA for the period of ten (10) years from inception or the date when it was last in effect, whichever is later. These include:

1. Compliance with notice requirements, by retaining copies of the notices issued by the Plan, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment.
2. Requests for access to PHI, request for confidential communication, requests for amendments or corrections to PHI, requests for accounting of disclosures, as well as requests for restrictions to use and disclosures of PHI and their disposition.

3. All complaints received, detail phases of the investigation process, and their disposition, if any.
4. All phases of the breach investigation process on a case-specific basis, in a manner sufficient to demonstrate that all appropriate steps were completed, including all supporting documentation associated with the potential breach.

DEFINITIONS:

Administrative Safeguards **–** Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Breach **–** the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI in that the disclosure of the information poses a significant risk of financial, reputational, or other harm to the individual.

Business Associate **–** A person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use of disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review and billing. The term Business Associates includes/also known as, FDRs (first-tier, downstream and related entities).

Covered entities **–** Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.

- *Health Care Provider* – Any provider of medical or other health care services or supplies who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard.
- *Health Plans* – Any individual or group plan that provides or pays the cost of health care (e.g., a health insurance issuer and the Medicare Program).
- *Health Care Clearinghouses* – A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice-versa.

Disclosure **-** any release, transfer, provision of access to, or divulging in any other manner of PHI to persons outside of the Health Plan.

Electronic PHI ("ePHI") **-** a subset of PHI that is created, received, maintained or transmitted in electronic format. All ePHI is Protected Health Information and is subject to the HIPAA privacy, security and breach notification requirements.

Physical Safeguards **–** Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Protected Health Information ("PHI") **–** means information, in any format, that is created or received by the Health Plan and relates to the past, present, or future physical or mental health or condition of a member; the provision of health care to a member; or the past, present, or future payment for the provision of health care to a member; and that identifies the member or for which there is a reasonable basis to believe the information can be used to identify the member.

Secured PHI **-** PHI that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals by either encryption or destruction by a method approved by the National Institute of Standards and Technology.

Technical Safeguards **–** Means the technology and the policy and procedure for its use that protects electronic protected health information and control access to it.

Unsecured PHI **-** any PHI that is not secured using one of the HHS-approved technologies or methods (encryption or destruction).

Use **-** the sharing, employment, application, utilization, examination, or analysis of PHI, in oral, written, electronic or other format.

Workforce member **–** includes employees, volunteers, trainees and other persons whose conduct, in the performance of work for a Business Associate, is under the direct control of the Business Associate.

☒ **Freedom Health** ☒ **Optimum HealthCare**	**Policy Title: Complaint Tracking Module** **Primary Department: Compliance** **Policy Number: COMP 12** ☒ **Medicare**
Approved By: Monique S. Akins 4.27.2020 Monique Akins *Manager, Compliance* *Date* Diane C.A. Kortsch 04.27.2020 Diane Kortsch *Staff VP Compliance* *Date*	**Create Date: 01/01/2008** **Effective Date: 01/01/2011** **Revision Date(s): 04/01/2012 – formerly COMP16; 04/01/2013; 04/01/2016; 04/11/2017; 12/14/18; 04/27/2020**
Reference: CTM SOP, CMS Prescription Drug Benefit Manual – Chapter 7 Section 70	

POLICY:

The Compliance Officer or authorized appointee is responsible for receiving and replying to all complaints reported in the Complaints Tracking Module (CTM) within the Health Plan Management System (HPMS) in accordance with CMS guidance.

The Compliance Officer or authorized appointee tracks the complaints, analyzes the data for trends and patterns and reports these findings at least quarterly to Senior Management Staff and the Board.

The Plan will strive to ensure timeliness with resolution of CTMs and work to continue to improve its efforts to keep CTMs to a minimum.

The Health Plan follows the standards designated in CMS' Complaint Tracking System Standard Operating Procedure (CTM/SOP).

PROCEDURE:

1. The Compliance Officer or authorized appointee, checks the Complaints Tracking Module (CTM) in HPMS numerous times on a daily basis including weekends.

2. Received complaints are entered into an internal central workflow system, called the CTM Module. The CTM module allows for appropriate CTM tracking across multiple departments.

3. Complaints are entered into the CTM Module with at least the following information:

    - Date the CTM was assigned to the Plan
    - Complaint ID number

- First and Last Name of Beneficiary
- HICN
- Contract
- Summary of Complaint
- Issue Level
- Due date

4. A timeframe for response to CMS is indicated depending on the Issue Level:

   - Immediate Need– 2 days

     CMS defines immediate need for MA as a complaint where a beneficiary has no access to care and an immediate need for care exists.

   - Urgent – 7 days

     CMS defines an urgent complaint (for MA) as one involving a situation where the beneficiary has no access to care, but no immediate need exists.

   - Non-Immediate Need/Non-Urgent – 30 days

5. Daily CTM report is provided to Senior Management team.

6. After initial investigation, the plan will enter preliminary documentation in HPMS case noted upon initial review. The plan will also provide updated documentation in HPMS not less than 24 hours of Immediate Need, three days for Urgent and five days for No issue level.

7. A determination is made by the CO or authorized appointee as to whether the Complaint was appropriately assigned to the correct Plan.

   - If the complaint should have gone to another Plan, the CO or authorized appointee indicates in the Complaint Resolution section - Casework notes, the name and/or contract number of the Plan to where the complaint should be reassigned and any additional pertinent notes related to the complaint A Plan Request is submitted.
   - In the Plan Request section- the CO or authorized appointee checks the option to indicate that this complaint belongs to another plan.

8. The complaint is entered into the Plan's CTM module for Department review. Departments are responsible to return their response to the CO or Designated Appointee.

9. The CO or authorized appointee reviews and determines if all information is submitted to appropriately respond to the Complaint. If it is not, additional information is requested from the department.

10. If the complaint needs CMS action to resolve, the CO or authorized appointee indicates in the Resolution/Casework section all pertinent information related to the complaint to support

the request and checks the option to indicate that this complaint is a CMS issue in the Plan Request section.

a. If the complaint is resolved, the findings, action and resolution are entered in Resolution Casework Notes. Dates and times of findings and actions are included. The Complaint is then closed following the procedures outlined in the CTM Plan SOP.
   - The Compliance department is responsible for ensuring the member is contacted to advise them of the resolution.
   - Per CMS' Best Practice standards, 4 attempts are made at different times. If the member cannot be reached, a letter unable to contact must be sent to the complainant.
   - The dates and times of each of these calls are documented.

b. If a resolution cannot be attained at this time, the findings and actions are reported to the Case Manager and the Complaint remains open until resolved. The resolution is reported and the member is contacted as above.

c. All complaints that require Retro Processing Contractor involvement are noted in the Resolution module and the complaint remains open until the enrollment issue is resolved. The date sent to the RPC will be documented in the case notes.

11. The Compliance Officer or authorized appointee keeps the involved department abreast of any further communication from the Case Manager until the case is closed.

12. The CO or authorized appointee ensures that every complaint is analyzed to determine the root cause. Complaints are also analyzed on a volume level to trends and patterns. These analyses enable the plan to identify opportunities for process improvement within the plan.

    a. The root cause analysis of each complaint includes but is not limited to:
       i. A review of calls made to the plan by the complainant/representative prior to the complaint being filed.
       ii. A review of member's account history (claims, authorizations, appeals & grievances) as applicable
       iii. If complaint involves an agent allegation, the plan reviews the agent's complaint history

    b. The root cause analysis of complaint volume includes but is not limited to:
       i. A review of provider/vendor complaint history
       ii. A review of Organizational/operational policies and procedures

13. The Compliance Officer or authorized appointee is responsible for preparing a summary report on all CTMs upon request to identify trends and patterns for Senior Management and regulatory requests as well as Quarterly reporting to the Compliance Committee. The Compliance Officer includes the analysis in quarterly reporting to the Board of Directors, the governing body of the plan.

☒ **Freedom Health** ☒ **Optimum HealthCare**	**Policy Title: Marketing and Member Material** **Primary Department: Compliance** **Policy Number: COMP 13** ☒ **Medicare**
Approved By: Monique S. Akins 4.27.2020 Monique Akins *Manager, Compliance* *Date* Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Staff VP Compliance* *Date*	**Create Date: 03/28/2012** | **Effective Date: 04/01/2012** **Revision Date(s): 03/28/2012; 04/01/2016; 04/11/2017; 12/14/2018; 11/11/2019; 04/27/2020** Incorporated previous COMP07, COMP08, COMP09, & former COMP13; 05/01/2013
Reference: Medicare Communications and Marketing Guidelines (MCMG); Section 1557 of the Affordable Care Act of 2010; Section 508 of the Rehabilitation Act of 1973	

POLICY:

All Marketing Materials, including any informational materials targeted to Medicare beneficiaries which promote the plan, that inform beneficiaries that they may enroll or remain enrolled in the plan, explain the benefits of enrollment into the plan, and/or explain how Medicare covered services are covered under the plan must be submitted file and use, or for review and approval by CMS with limited exceptions. The Compliance Officer, or designee, will serve as the liaison between the Health Plan and CMS to ensure compliance with approval of materials with limited exception.

The Health Plan complies with the CMS guidelines to ensure beneficiaries who join the plan are protected against any benefit changes. Except for CMS approved benefit enhancements, the plan will not make any benefit changes during the contract year. If changes are required, notice of change will be sent to affected beneficiaries 30 days prior to the effective date of the changes.

The Health Plan does not discriminate based on race, ethnicity, national origin, religion, gender, age, mental or physical disability or geographic location within the service areas and ensures services are carried out to beneficiaries in a culturally competent manner.

The Health Plan makes available all required marketing and member materials in any language that is the primary language of more than 5% of the plan's benefit package service area and has the required material available on the plan website. The plan offers interpreter services through the member service call center utilizing a contracted language interpreter service as well as TTY/TDD services for all current and prospective members. The Health Plan complies with Section 508 of the Rehabilitation Act regarding the plan's internet website technology and information standards for people with disabilities in addition to other requirements as specified in the Act.

All communications (letters, newsletters, materials, scripts, etc.) that will either be sent to or directly affect any Health Plan Member or Provider must be forwarded to the Compliance Officer for review before it is published.

Marketing for an upcoming plan year may not occur prior to October 1. The Health Plan will cease current year marketing activities once they begin marketing benefits for the new contract year. Prior year materials may be provided upon request and enrollment applications may be processed.

The Health Plan prohibits advertising outside of its defined service area unless such advertising is unavoidable. For situations where this cannot be avoided, (e.g., advertising in print) the Health Plan will clearly disclose the service area in the marketing materials.

The Health Plan will post all required Plan documents in accordance to CMS Medicare Marketing Communications and Marketing Guidelines (MCMG); and all other State and Federal requirements.

PROCEDURE:

The Compliance Officer or designee reviews all marketing/member materials prior to upload in to CMS's HPMS system and/or distribution to ensure enforcement of requirements as outlined in the Medicare Communications and Marketing Guidelines (MCMG). Compliance reviews consist of, but are not limited to:

- Ensuring plan materials meet anti-discrimination requirements, Materials & Marketing:
    - Do not discriminate based on race, ethnicity, national origin, religion, gender, age, mental or physical disability, health status, claims experience, medical history, genetic information, evidence of insurability, or geographic location.
    - Do not target beneficiaries from higher income areas or state/imply that plans are only available to seniors rather than to all Medicare beneficiaries unless the plan is a Dual Eligible Special Needs Plan (D-SNP). Only Special Needs Plans (SNPs) may limit enrollments to individuals meeting eligibility requirements based on health and/or other status. Basic services and information must be made available to individuals with disabilities, upon request.

- Ensuring Non-English speaking population requirements are met.
    - Required marketing materials, as outlined in the MCMG, are made available in any language that is the primary language of at least five (5) percent of the Health Plan's benefit package service area.
    - The Health Plan contracts with language translators to accurately translate required member material (when required by Federal, State, or other Regulatory Agencies). The Plan is not required to submit non-English language materials that are based on an English version. If the Plan creates a material to be used only in a non- English language, the Plan will submit an English translation to HPMS. The Plan will submit multi-lingual marketing materials that include English and another language (or languages). The Plans will include a note in the comments field specifying that the material is multi-lingual.

- Ensuring all Section 1557 requirements are met.
    - The Plan will take steps to notify beneficiaries, enrollees, and prospective members about their rights under Section 1557 and our obligations under Section 1557.
    - The Plan will post a nondiscrimination Notice in English and post taglines in at least the top 15 non-English languages spoken by individuals with limited English proficiency of the relevant State or States.
    - The Notice and Taglines will be posted in a conspicuously-visible font size in a conspicuous location of covered entity websites accessible from the home page, in significant communications and significant publications, and, where appropriate, in conspicuous physical locations where the entity interacts with the public.
    - For significant communications and significant publications that are small-size, such as trifold brochures, the Plan will post a nondiscrimination statement and taglines in at least the top 2 non-English languages spoken by individuals with limited English proficiency of the relevant State or States.
    - If the five (5) percent service area threshold is applicable to a language not currently in the top 15 languages spoken by individuals with limited English proficiency in the relevant State or States, the Plan will add that particular language to the multi-language insert.

- Ensuring marketing materials and member materials contain appropriate Marketing Identification as outlined in the MCMG (with exceptions noted in the MCMG).

- Ensuring proper hours of operation and contact information (inclusive of Plan Name, phone number, websites, and TTY numbers)
        - An accurate toll-free number must be listed
        - The Health Plan's member service call center hours are the same for all individuals regardless of whether they speak another language or use assistive devices for communication.
        - ID cards and the standardized Star Ratings document are excluded from this requirement
        - A toll-free TTY number also appears in conjunction with the Member Services number in the same font size and style as the other phone numbers.
    - Organization Names and Plan name are correct
    - Addresses are correctly listed
    - Websites are displayed appropriately

- Ensuring proper use of contracting statements and applicable disclaimers
    - Disclaimers are prominently displayed on the material and must be of similar font size and style.
- Ensuring "Use of proper Font size and logos"
    - All text included on materials, including footnotes, is printed with a font size equivalent to or larger than Times New Roman twelve (12)-point (unless otherwise noted in the MCMG). The equivalency standard applies to both the height and width of the font.

    - Logos are prominently displayed on the material and must be of similar font size and style.
- Ensuring Compliance with Section 508 of the Rehabilitation Act of 1973
    - Review conducted with assistance of the Plan's Information Systems & Information Technology departments ensures effective communication with individuals with disabilities and to provide auxiliary aids and services, such as alternate formats (e.g., braille, audio, large format), to individuals with disabilities to ensure an equal opportunity to access the agencies' programs.
    - The plan will post on the internet the required translated material. The company uses software designed to detect 508 compliance within website material. The IS Department will run a verification check of website material through the software and report to the Compliance Department any deficiencies.

The material is uploaded through the Marketing Module of the HPMS system by the compliance area upon approval from the Compliance Officer or designated staff. When the Health Plan chooses to modify the model language, it must ensure that all elements provided in the model are included in the non-model document. The Plan will remove any reference to the words; "exhibit", "model", or "appendix" used in the title of the model document form the title of the non-model document. Upon upload of materials, the compliance area will communicate the level of CMS review the submitted material require to the business area. Unless specifically requested to do so by CMS, the Plan will not submit Communication materials into HPMS.

Time Frames for Marketing Review:

1. File & Use - submit eligible marketing materials in HPMS at least five (5) calendar days prior to their distribution.
2. Standardized Model - results in a 10 day marketing review period or it may be submitted via File & Use.
3. Non-Standardized model "Non-Model" – may result in that material being subject to a 45-day review period.

Upon CMS' approval or acceptance of the uploaded material, the Compliance Officer or designee communicates with relevant staff for distribution. The material status is not utilized with the Material ID.

If there are any changes or corrections made to final materials (e.g., the benefit or cost-sharing information differs from that in the approved bid), the Health Plan will correct those materials for prospective enrollees and may be required to send errata sheets/addenda/reprints to current members.

☒ **Freedom Health** ☒ **Optimum HealthCare**	**Policy Title: Agent/Broker Oversight** **Primary Department: Compliance** **Policy Number: COMP 14** ☒ **Medicare CCP**
Approved By: Monique S. Akins 4.27.2020 Monique Akins *Manager, Compliance* *Date* Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Staff VP Compliance* *Date*	**Create Date: 09/01/2012** **Effective Date: 09/01/2012** **Revision Date(s): 04/01/2016; 04/11/2017; 12/14/2018; 04/27/2020; Incorporated COMP 03, COMP 06, COMP07**
Reference: Medicare Communications and Marketing Guidelines (MCMG); 42 CFR 422.2272; 422.2274; 423.2272 & 423.2274	

POLICY:

The Health Plan has developed a Marketing Oversight Policy (MOP). The MOP is designed to prevent prohibited marketing practices from occurring, to detect prohibited marketing tactics at their early stages, and to take immediate corrective action to respond to aggressive and misleading marketing tactics. The MOP is also designed to promote adherence to appropriate standards of business conduct throughout all aspects of the organization's marketing and sales operations and to ensure conformance with applicable federal, state, and local statutory and regulatory obligations (e.g., Medicare Improvements for Patients and Providers Act (MIPPA) by the organization and its employees (executive, management, and support staff), partners, vendors, marketing employees, independent agents, independent brokers and its delegates (first tier entities, downstream entities, and related entities).

The components of the MOP include:

- Compliance Department ownership of the Marketing Oversight Policy;
- Compliance with agent appointment regulatory requirements;
- Agent/Broker Training;
- Agent and Broker Complaints and Investigation Process
- Implementation of an internal secret shopper program;
- Implementation of Disciplinary Actions

PROCEDURE:

A. Compliance Department Ownership of Marketing Oversight Policy

The Plan's Compliance Department and Compliance Officer is responsible for implementing and monitoring the policy in close coordination with the other departments.

- The Compliance Department assists the In-house Legal Counsel in preparing the Agents/Broker contracts to ensure that all CMS requirements have been incorporated in the contracts, including all compensation structure, the beneficiary contact restrictions, the solicitation restrictions and telephone call restrictions.
- The Compliance Department works with the Sales Operations Department to ensure that all agents/brokers are trained and all CMS guidelines and memos are made available to agents/brokers
- The Compliance Department works with the Sales Operations Department to analyze the member cancellation/disenrollment data and commission charge backs on a periodic basis to identify trends relating to specific agents/brokers.
- The Compliance Department oversees a comprehensive internal secret shopper program of all Plan sales events and seminar presentations utilizing both outside vendors as well as in-house staff.

A periodic report on the marketing oversight activities are presented to the Compliance Committee on a quarterly basis

B. Compliance with Agent Appointment Regulatory Requirements

The Plan requires Operations and Field Sales Management to utilize only state licensed individuals, who have been trained and successfully certified by the Plan in both general Medicare topics and Plan specific products information to market the organization's Medicare plans. This requirement of state licensure and good standing status apply to employed agents, contracted downstream independent brokers/agents and downstream brokers/agents of contracted Field Marketing Organizations (FMOs). The following are the requirements for agent/brokers to sell the Plan's products:

- All employed agents, independent brokers/agents and downstream brokers/agents of FMOs have individual hard copy or electronic personnel files. These files are maintained by the Sales Operations Department.
- All employed agents, contracted downstream independent brokers/agents and downstream brokers/agents of contracted FMOs are required to complete a "Pre-Test Compliance Questionnaire and Attestation".
    - The Compliance Questionnaire and Attestation requires employed agents, independent brokers/agents and downstream brokers/agents of FMOs to attest to their past sales compliance history, criminal and civil background history, attest to their commitment to compliance with the Plan and to attest to their compliance with the use of approved Plan sales presentation(s) and material(s). They also attest to reading and understanding the CMS Marketing Guidelines and the HIPAA Business Associate Agreement.

- All employed agents, independent brokers/agents and downstream brokers/agents of FMOs are provided a copy of the current CMS Marketing guidelines at the time of employment agreement or contracting, whichever is applicable.
- A signed acknowledgment form is received from the employee/agent/broker. Managers of employed agents and managers of FMOs and general agencies are also provided a PDF version of the current year's marketing guidelines.
- Employed agents, independent brokers/agents and/or downstream brokers/agents of FMOs require an annual certification to be able to continue to write business.
- To qualify for certification, an employee/agent/broker are required to complete and pass a test that includes questions on general Medicare topics, marketing compliance topics, and Plan specific benefit topics. The employee/agent/broker has to score at least 85% or better to be certified to sell.
- Test results are made part of the employee/agent/broker hard copy or electronic file.

C. Agent and Broker Training

All employed agents, independent brokers/agents and downstream brokers/agents of FMOs receive annual training on Medicare rules, regulations, and plan details specific to the products being sold by the agents/brokers. As part of the training and education, brokers and agents are tested annually. To comply with the requirement:

- The Compliance Department in correlation with the marketing area prepares an agent training module incorporating all the CMS guidelines, HIPAA requirements, state insurance requirements, and plan specific products;
- Agent/Broker training is conducted according to Plan's Marketing Policy.
- Presenter training is prepared by sales/marketing management group and reviewed and approved by compliance. Approved presenter training is administered by the Sales/Marketing group. It is provided in a classroom setting. Agents/Brokers must take a written test. In addition, each presenter must prepare a mock presentation in front of a panel of three designated subject matter experts and must obtain a consensus for passing. Only certified presenters are allowed to present at seminar/sales events.

D. Agent and Broker Complaints and Investigation Process

The Compliance Department develops and implements mechanisms to monitor and investigate complaints of marketing misrepresentation by agents and brokers. Complaints against agents and brokers may be received from various sources, including:

- *External*
  - CMS Complaints Tracking Module (CTM)
  - Florida State Department of Financial Services service requests
  - Other State/County agencies like Better Business Bureau and Consumer Protection Departments
  - State/Federal Congressional Offices
- *Internal*
  - Calls received by the Plan's Member Services Department
  - Calls received by the Plan's Appeals/Grievances Department
  - Correspondence received by the Plan
  - Post-Enrollment Verification Calls
  - Disenrollment/Cancellation Quality Improvement Calls

The Health Plan's Compliance Department reviews and investigates all complaints that involve allegations of agent misconduct selling the Company's products. The Compliance Department takes appropriate disciplinary/corrective actions against agents based on the findings of its investigations. The investigation process includes:

1. **Logging the complaint.** When a complaint has been received by the Compliance Department against an agent/broker, the complaint is first logged into the Compliance sales and marketing investigations log.
2. **Determine severity of complaint.** Determine if complaint warrants an expedited investigation. Expedited cases are those in which the beneficiary's complaint indicates their life or health is in jeopardy due to the agent's reported misconduct. Expedited cases are investigated within 24-48 hours from receipt.
3. **Initiating the investigation.** All investigations are initiated within 14 calendar days of receipt, unless an expedited review has been determined.
4. **Researching the complaint.** Before making any agent/broker and/or beneficiary contact, the Compliance Department researches internal and external systems for agent and beneficiary information. This includes verifying the agent(s) involved in the complaint. The case files and tracking log may include the following items:
   a. Beneficiary application and other enrollment documentation such as the Scope of appointment (SOA) and/or Voice recorded appointment (VRA)
   b. Beneficiary detail from Plan System
   c. Beneficiary call detail
   d. Agent license verification via the appropriate DOI site
   e. Agent complaint history
   f. Agent trainings and certification, including dates, methods and results for each

5. **Contact the beneficiary.** There may be instances when the beneficiary needs to be contacted for additional information. When contacting beneficiaries, Compliance asks them to explain their experience with the agent. Three attempts are made to contact the beneficiary. All attempts are documented, including the time and date of each attempt and whether or not a message is left for the beneficiary to return the call. The call with the beneficiary is documented in the case file and/or tracking system.

6. **Contact the agent/broker.** Request a written statement from the agent. The agent's cooperation is expected and required by the Health Plan during the investigation of the complaint. Failure to respond to the request(s) for information will result in disciplinary/corrective action, including suspension or termination of the agent's ability to sell the Company's products.

7. **Review of the agent's statement and case file.** Once statement has been received, Compliance reviews the agent's statement and the case file. If additional information is needed, the agent is requested to provide additional details. Again, depending on the severity of the complaint, the agent is provided with the appropriate timeframe to respond.

8. **Resolution of investigation.** Upon resolution of the investigation, all case notes are documented and finalized in the sales and marketing log.

9. **Compliance Communication:** All cases are presented to the compliance committee and Board of Directors on a quarterly basis.

The Compliance Department analyzes the data from internal and external sources related to agent/broker complaints and identifies those brokers/agents that have multiple complaints. These cases are documented and reported to Senior Management for termination of broker/agent contracts or for additional training/corrective action.

E. Internal Secret Shopper Program

The Plan has implemented an internal secret shopper program as one of its methods for providing Sales & Marketing monitoring and oversight. The secret shopper program is comprised of observations designed to solicit information on the sales and marketing activities conducted by agents and brokers contracted by the Health Plan. This program aids in identifying areas of opportunities for coaching and training; and assurance of compliance with Medicare Marketing Guidelines and the Plan's policies.

- The Compliance Department utilizes an external secret shopper agency to perform secret shops of the Plan's formal seminars/sales events.
- The Compliance Department prepares a standard evaluation tool, similar to CMS' surveillance tool, for the secret shoppers to document their findings and comments.
- A list of sales events and sales seminars are selected from the sales events and sales seminar data uploaded to CMS.
- For each event, secret shoppers are tasked with observing the presenter (an agent/broker), other plan representatives, marketing materials, and the venue. The Compliance Department receives a report of the shopper's observations.

- The evaluations completed by the secret shoppers are transmitted to and received daily by the Plan.
- Each secret shop report is reviewed by dedicated resources within the Plan's Compliance department for Sales & Marketing monitoring and oversight purposes; as well as, a tool in providing operational and venue feedback to the Sales & Marketing management.
- Findings from each report are discussed in a cross-functional meeting and corrective action plans are implemented when appropriate.
- Compliance area requires these corrective actions to be implemented immediately and all back up documentation is housed in a central location.

F. Disciplinary Actions

The Plan is responsible for the oversight of all downstream marketing and sales activities of an employee of the Plan, an independent agent, an independent broker or other similar managerial marketing position intended to affect a beneficiary's choice among Medicare plans. Substantiated violations could result in the form of written correction up to and including termination and reporting to the State Department of Insurance and/or other government agencies. All final corrective actions, determinations and recommendations for corrective actions are contingent upon the severity of the infraction and it may include a review of the agent's file (including complaints, all enrollments, cancellation/disenrollment, etc.).

Following an investigation of an agent/broker compliance issue where a case is confirmed substantiated, the Compliance Officer, or authorized designee determines appropriate disciplinary action. Following, are the steps of the disciplinary action (also referred to as corrective 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. The level of disciplinary intervention may also vary. Some of the factors that are considered depend upon the nature of the compliance violation and the risk the violation poses to Plan enrollees. Other factors include, but are not limited to, whether the offense is repeated despite counseling and/or training and the employee's history with compliance related issues, if any.

Results of the investigation may result in the following disciplinary actions;

1. Manager-coaching
2. Manager Ride-a-longs
3. Re-training
4. Documented Verbal/Written Warning
5. Suspension
6. Termination
7. Notification to the State, CMS, and/or Medic or other appropriate agency

☒ Freedom Health, Inc. ☒ Optimum HealthCare	**Policy Title: Records Retention** **Primary Department: Compliance** **Policy Number: COMP 15** ☒ **Medicare**
Approved By Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Staff VP Compliance* *Date*	**Create Date: 09/01/2012** **Effective Date: 09/01/2012** **Revision Date(s): 04/01/2016; 04/14/2017; 04/27/2020**
Reference: 42 CFR 422.504(d); 42 CFR 422.504(e); Medicare Managed Care Manual, Chapter 11, 110.4.3;; Medicare Managed Care Manual Chapter 21; CMS Prescription Drug Benefit Manual Chapter 9.	

POLICY:

The Health Plan has established this Records Retention Policy which governs the retention, maintenance, and proper disposition or destruction of the Plan's documents and records in accordance with State and Federal laws and related regulations.

This policy applies to all directors, officers, employees, contractors, first tier, downstream and related entities, volunteers and consultants of the Plan (collectively referred to herein as "Associates").

Federal law provides that the Department of Health and Human Services (DHHS), the Comptroller General, or their designees may audit, evaluate or inspect any books, contracts, medical records, patient care documentation and other records of the Plan (including that of any related entity, Statewide Managed Medicaid The Plan further extends this right to State regulatory agencies.

Associates must maintain any and all books, contracts, medical records, patient care documentation, plan records and documents:

- Records sufficient to accommodate periodic auditing of the financial records (including data related to utilization, costs, encounter data, and computation of the bid proposal).
- Records sufficient to enable CMS and the Agency to inspect or otherwise evaluate the quality, appropriateness and timeliness of services performed under the contract and the facilities of the organization;
- Records sufficient to enable CMS to audit and inspect any books and records of the MA organization that pertain to the ability of the organization to bear the risk of potential financial losses, to services performed, or determinations of amounts payable under the contract;

- Records sufficient to properly reflect all direct and indirect costs claimed to have been incurred and used in the preparation of the bid proposal;
- Records sufficient to establish component rates of the bid proposal for determining additional and supplementary benefits;
- Records sufficient to determine the rates utilized in setting premiums for State insurance agency purposes, and for other government and private purchasers;
- Records relating to ownership and operation of the MA organization's financial, medical, and other record keeping systems;
- Financial statements for the current contract period and 10 prior periods;
- Federal income tax or informational returns for the current contract period and 10 prior periods;
- Asset acquisition, lease, sale, or other ownership issues;
- Agreements, contracts, and subcontracts;
- Franchise, marketing, and management agreements;
- Schedules of charges for the MA organization's fee-for-service patients;
- Documentation of matters pertaining to costs of operations;
- Documentation of amounts of income received by source and payment;
- Cash Flow statements; and
- Any financial reports filed with other Federal programs or State authorities;

Additionally, for purposes of this policy, the Plan sets forth specific guidelines regarding other documents, records, and data of the Plan which includes: all written, printed, typed, recorded or graphic matter of every type or description including, but not limited, to minutes of meetings, investigatory documentation, authoritative documentation, corrective action plans, educational materials, financial records, enrollment and disenrollment records, business agreements/contracts, and records to evaluate the quality, appropriateness, and timeliness of services furnished to enrollees, instructions, directives, reports, notes, lists, memoranda, correspondence, agreements, charts, graphs, spreadsheets, manuals, videotapes, audiotapes, data compilations, marketing materials, training materials, and material stored in any data storage system, including electronic mail and electronic formats. Such documents, records and/or data include those maintained in hardcopy files and those received, created, sent, or maintained in electronic files on computer systems, computer hard drives, removable media (*e.g.*, CDs and DVDs), flash drives, laptop computers, company issued PDAs and smartphone devices, and includes electronic archives, back-up tapes, and/or disaster recovery tapes.

All Associates are responsible for:

A. Preserving all aforementioned documents and records in accordance with the Plan's retention requirements contained herein.

B. Maintaining records in a safe storage area that promotes efficient retrieval and maintaining personal papers and non-record materials separately from official Plan records.

C. Neither destroying nor removing records (whether physically or electronically) from the Plan's facilities without authorization from the Compliance Officer and/or Corporate Counsel.

If an Associate is unsure whether certain documents or information should be preserved, err on the side of caution and preserve the information. If there are further questions with how to comply with this policy, please contact the Compliance Officer and/or Corporate Counsel.

PROCEDURE:

A. *Records Maintenance:* The Health Plan maintains all training records for a period of 10 years of the time, attendance, topic, attestations and test scores of any tests administered to their Associates and also require FDRs to maintain records of the training of the FDRs Associates. The Plan maintains compliance violation disciplinary actions, date violation was reported, description of the violation, date of the investigation, summary of findings, disciplinary action taken and the date it was taken for a period of 10 years.

B. *Records Retention Schedule:* All Plan documents and records created in accordance with the operation of the Plan, will be maintained for a minimum of ten (10) years from the end date of the Plan's contract or the completion date of an audit, whichever is later unless:

1. CMS determines there is a special need to retain a particular record or group of records for a longer period.
2. There has been a termination, dispute, or fraud or similar fault by the Plan, in which case the retention may be extended to six years from the date of any resulting final resolutions of the termination, dispute, or fraud or similar fault; or
3. CMS determines that there is a reasonable possibility of fraud, in which case it may inspect, evaluate, and audit the Plan at any time.
4. There is ongoing litigation or internal or external investigations, lawsuits or similar actions, then records relevant to the action shall be retained until the action is concluded, in accordance with applicable statutes, regulations, and Plan policy.

C. *Method of Retention:* To the extent practicable, records will be maintained in a form to be designated by the Plan provided that such format allows for the accurate reproduction of such records.

1. Each business area will maintain a centralized list and description of its official records, filing procedures, and filing techniques of official records.
2. The Plan will maintain electronic records according to a specified file structure within the designated network drive.
3. The Plan will archive hard copy records, when electronic format is not feasible, at a pre-determined records retention facility.

D. *Access to Records:* The Plan allows access to DHHS, the Comptroller General, or their designee to Plan facilities and records to evaluate through inspection or other means:

- The quality, appropriateness, and timeliness of services furnished to Medicare/Medicaid enrollees under the contract;
- The facilities of the MA organization; and
- The enrollment and disenrollment records for the current contract period and 10 prior contract periods.

E. *Record Destruction:* Records will be destroyed, in a manner set forth by the Compliance Officer in consultation with the Legal department, upon the expiration of the retention period. If at the expiration of the retention period, there is any litigation or any internal or external investigation, then records relevant to the action will be retained until the action is concluded, in accordance with applicable statutes, regulations, and Plan policy.

1. Only documents and records which do not contain an original signature and have been previously preserved in electronic format may be disposed of or placed in shredder bins. The Compliance Officer and Corporate Counsel, in consultation, must provide written authorization for the destruction of records.
2. Authorization for record destruction will be documented, including the date/time of disposal, the name and title of the individual providing authorization, and a description of the type of record(s) destroyed.

F. *Disciplinary Actions:* The Compliance Officer and/or Corporate Counsel will investigate suspected violations. Each action is considered on a case-by-case basis and disciplinary actions are imposed on a fair and equitable basis and consistently applied. Appropriate sanctions are instituted against Associates who fail to comply with the Plan's Record Retention policies and procedures contained herein. The Plan maintains a separate policy and procedure for Disciplinary Actions.

G. *Penalties:* Knowingly destroying or altering documents with the intent to obstruct a pending or anticipated official government proceeding is a criminal act and could result in large fines and incarceration.

☒ Freedom Health, Inc. ☒ Optimum HealthCare	**Policy Title: Conducting Oversight of First Tier, Downstream and Related Entities (FDRs)** **Primary Department: Compliance** **Policy Number: COMP 16** ☒ **Medicare**
Approved By: Krista Gibbons *Date* *Manager, Delegation Oversight* Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 09/01/2012** **Effective Date: 09/01/2012** **Revision Date(s): 05/02/2016; 07/20/2017; 01/02/2019; 04/27/2020**
Reference: Medicare Managed Care Manual Chapter 11; CMS Prescription Drug Benefit Manual Chapter 9; Medicare Managed Care Manual Chapter 21; 42 CFR §§ 422.503(b)(4)(vi)(C), 423.504(b)(4)(vi)(C), and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG").	

POLICY:

The Health Plan by written contract may enter into contracts with First Tier Downstream and Related Entities (FDRs) to provide administrative or health care services to enrollees on behalf of the sponsor. The Health Plan maintains the ultimate responsibility for fulfilling the terms and conditions of its contract with State and Federal Regulatory Bodies including ensuring services are performed in compliance with all rules, regulations, program requirements and accreditation standards. The purpose of this policy is to ensure that our First Tier, Downstream and Related Entities are in compliance with all applicable federal and state laws, rules and regulations, Federal Health Care Programs and the Corporate Integrity Agreement.

PROCEDURE:

Identification of FDRs

The Health Plan has established an FDR Committee that is comprised of the Compliance Officer, Legal Counsel and Compliance personnel. The FDR Committee reviews and analyzes the below criteria to evaluate and determine the classification of an entity as an FDR.

The following factors listed below are taken into consideration when determining whether an entity is an FDR:

- The function to be performed
- Whether the function is something the Health Plan is required to do or to provide under its contract with federal and state regulations
- To what extent the function directly impacts enrollees
- To what extent the entity has interaction with enrollees, either orally or in writing
- Whether the entity has access to beneficiary information or personal health information
- Whether the entity has decision-making authority (e.g., enrollment vendor deciding time frames) or whether the entity strictly takes direction from the Health Plan
- The extent to which the function places the entity in a position to commit health care fraud, waste or abuse
- The risk that the entity could harm enrollees or otherwise violate Medicare Program Requirements or commit FWA

Risk Assessments, Monitoring and Audit Work Plan, and Corrective Actions

An effective monitoring and auditing program begin with a comprehensive First Tier Risk Assessment. Since risks change and evolve with new regulations, program requirements and operational changes, the Plan performs a comprehensive annual risk assessment and conducts an ongoing review throughout out the year to identify and address risks associated with the plan's participation in Federal Health Care Programs and the Corporate Integrity Agreement. In order to establish an effective system for monitoring and auditing, the Plan utilizes a Compliance Risk Assessment Matrix that considers the entity's nature of services performed, past performance, open corrective action plans, financial and Stars Impact including any regulatory notices of non-compliance. The weight for each risk metric is calculated into an aggregate risk score ultimately assigning an overall risk rating level. The baseline risk assessment results rank and prioritize those FDRs that potentially pose the greatest risk to the Plan's Compliance Program including all regulations associated with the plan participation in the Federal Health Care Programs. The following risk levels are utilized to prioritize the risks:

High	Occurs when a practice, process or procedure has been identified as non-functional/non-productive, noncompliant and/or has high impact or risk organizationally or to a beneficiary.
Medium	Occurs when an issue, process, etc. has been remediated; however, the issue, process, etc. poses a potential impact compliance risk, organizationally or to the beneficiary.
Low	Occurs when risk results from new state/federal regulatory guidance that has been released or the risk identified is a minimal impact compliance risk, organizationally or to the beneficiary.

The Risk Assessment results are reviewed with Executive Management and ongoing updates are presented at least quarterly to the Compliance Committee and Board of Directors.

The Plan then selects a reasonable number of First Tier Entities, develops and implements the monitoring and audit work plan, conducts audits and monitoring activities, and ensures the results of the Risk Assessment and corrective action plans are implemented and tracked to mitigate all organizational risks.

The Work Plan consists of the FDR, function/activity being audited/monitored, date efforts began, scope of monitoring/audit activity (what is being measured), audit objectives/scope, audit type (announced vs. unannounced, desk audit vs. onsite), schedules (including start and end dates), status (scheduled, open or closed), audit/monitoring findings/outcomes, as well as a description of any corrective/remediation action taken as a result of the activity conducted (audits, report analysis and/or sample reviews).

The Oversight Team reviews and confirms such compliance against Medicare regulations, sub-regulatory guidance, program requirements, contractual agreements, and all applicable Federal and State laws.

Monitoring Process

Monitoring activities are ongoing reviews performed of the Plan's FDRs operations to confirm continued ongoing compliance with State and Federal regulations, sub-regulatory guidance, and contractual agreements to ensure that corrective actions are undertaken and effective when issues are detected.

All functional areas are required to monitor their FDRs and report any risks or identified issues of non-compliance to the Compliance Committee. If risk items are identified Compliance may conduct adhoc focused or targeted audits. If warranted and depending on the severity, corrective actions may be issued and are tracked on the work plan.

Typical reporting received by the Health Plan may include but is not limited to:

- Claims payment reports
- Provider network adequacy
- Call center statistics
- Utilization statistics
- Credentialing/Recredentialing Statistics

Audit activities are formal reviews performed of the FDRs operational areas to test compliance with a particular set of standards (e.g., policies and procedures, laws and regulations) used as base measures for the functions that are delegated on behalf of the Plan. The Health Plan conducts both desk and on-site audits. Some of the factors that will determine whether a desk audit or on-site audit will be conducted include the size of the entity, complexity of work, and the areas of concern identified in the risk assessment.

For core functions that are delegated, the Plan evaluates the entity's ability to perform the delegated functions/services by evaluating the regulatory requirements that are applicable as well as the potential risks should they fail to perform in a compliant manner.

If entity is approved for delegation, a Delegation Agreement is executed outlining the detailed roles and responsibilities, specifying the delegated activities, responsibilities and reporting, the process by which

the Plan conducts formal evaluation of the entity's performance at least annually, the remedies available if the entity does not fulfill their obligations or performance is inadequate including corrective actions, revocation and/or termination.

Delegation of activities may be suspended, revoked and/or terminated when a Governmental Authority determines that an entity has not performed satisfactorily, including failing to implement a corrective action plan, or termination of the Delegation Agreement at any time for cause related to egregious deficiencies.

Audit Process

FDR audits are conducted utilizing the following methodology:

1. *Audit planning*
    a. Audit activity selected based on audit work plan.
    b. Regulatory Requirements are outlined in the Delegation Operational Audit Tools
    c. Focused or Adhoc audit may be based on risk criteria, such as new or updated regulatory guidance, reports of compliance issues, etc.
    d. Audit notification – Notice includes, activity audited, audit objectives/scope, universe specifications and due date for universe data, and any other required documentation (policy & procedures, step actions).

2. *Audit Initiation*
    a. Send out the audit notification which includes universe time frame and sample selections
    b. Analyze the universe and select samples
    c. Samples are selected based on aberrant behavior, targeted sampling, or the NCQA audit methodology - 5% or 50 files or 8/30 Audit Methodology

3. *Deficiencies* - Identified deficiencies may result in one of the following:

    Corrective Action Required (CAR) – A CAR is the result of a material non-compliance with specific requirements that does not have the potential to cause significant beneficiary harm.

    Immediate Corrective Action Required (ICAR) - An ICAR is the result of non-compliance with specific requirements that has the potential to cause significant beneficiary harm.

    Observations- are either immaterial events of non-compliance with specific requirements or other items that may be useful to management in preventing contract non-compliance in the future (i.e. isolated human error). Observations may require follow up actions.

4. *Audit Report Preparation*

Document the audit results in an audit report which includes: the audit objective, scope and methodology, findings, recommendations and corrective actions, if issued.

5. *Notice the FDR*

   Upon identification of deficiencies and/or completion of audit, approved formalized audit results and/or corrective action plan is sent to the first-tier entity and the business owner. If any deficiencies identified, will obtain FDR response which shall include root cause, member impact analysis and timeline for remediation.

6. *Close Audit*

   a. Audit work plan is updated

   b. Required follow-up/validation reviews are added to audit/monitoring work plan

   c. Audit results and any corrective actions are presented to the Delegation Oversight Committee, Quality Management Steering Committee, Compliance Committee, and the Board of Directors on a quarterly basis.

7. *Validation Audits*

   a. An auditor performs the CAP validation review/follow-up review as a separate audit on the audit work plan.

   b. For remediated deficiencies, Compliance will review, approve and close the CAP

   c. For non-remediated deficiencies, Compliance will require additional monitoring and auditing activities until the deficiency is remediated and/or termination of contract depending on risk and impact to beneficiaries

   d. Periodic reviews are conducted to confirm ongoing compliance and to ensure corrective actions have been effective and remediated

8. *Regulatory Notification*

   Regulatory Agencies are notified prior to the effective date of the delegated activities as required below:

   Medicare- Changes to First Tier/Downstream/Related Contracts (FDR) for Key Part C and Part D Functions require sixty (60) day notification to the CMS Account Manager prior to the effective date of the new contract.

The Delegation Oversight Committee (DOC) is comprised of key leadership across the organization including but not limited to senior level executives and meets at least quarterly. In addition, the delegation audit and monitoring oversight activities and findings are also reported to the Compliance Committee and Quality Management Steering Committees at least quarterly. The activities and findings are also presented to the Board of Directors.

Communication and Information Exchange

The Health Plan maintains well established lines of communication with our contracted First Tier, Downstream and Related Entities. The Plan conducts formal and informal meetings as well as verbal and written communications where we share information such as training materials, audit protocols, best practices, job aides, changes in statutory and federal regulations (HPMS memos), policies and procedures, change in processes that may impact delegated activities, performance issues, compliance concerns, and/or periodic updates to ensure the Plan and the FDRs maintain their commitment to comply with all applicable federal and state laws, rules and regulations and to avoid notices of non-compliance and regulatory penalties.

Distribution of Standards of Conduct and Compliance Policies and Procedures

The Health Plan communicates compliance expectations through distribution of the Plan's Compliance Policies and Procedures, Compliance Plan and Standards of Conduct. These documents are made available and distributed through the Compliance-Provider/Vendor Training System and via email communications at the time of contracting (within 90 days), when there are material changes, and annually thereafter. Those FDRs selected for audit are evaluated to ensure they have comparable Compliance Policies and Procedures, Standards of Conduct that are distributed to employees and First Tier, Downstream Related Entities as required by regulations.

Corporate Integrity, Compliance Program, Federal Healthcare Program Anti-Kickback Statute and Stark Law Training Requirements

The Plan provides all covered persons annual training regarding the Plan's Corporate Integrity Agreement requirements, Compliance Program, Federal Healthcare Program requirements including the Anti-Kickback Statute and the Stark Law.

For the purpose of the CIA Covered persons include all contractors and subcontractors. Covered persons do not include active Medicare providers who are not employees of the Plan.

FDRs selected for audit are evaluated to ensure they have FWA and Compliance Training & Education.

OIG/GSA Exclusion

FDRs must review the HHS Office of the Inspector General (OIG) List of Excluded Individuals and Entities (LEIE) and the US General Services Administration (GSA) Excluded Parties List Systems (EPLS) exclusion lists 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.

FDRs must remove any individual or entity from responsibility or involvement with the Plan operations related to Federal Health Care Programs that are found to be excluded from participation or have been convicted of a criminal offense that falls within the scope of 42 U.S.C 1320a-7 (a) but has not yet been excluded.

In addition, FDR employees, board members, officers, vendors, contractors or first tier downstream, related entities must immediately disclose if they, or upon discovery, another employee becomes subject to exclusion. FDRs should have disciplinary actions for those who do not comply with this obligation.

Those FDRs selected for audit are evaluated to ensure evidence of OIG/GSA exclusion screenings are conducted prior to hire and monthly thereafter.

Annual FDR Attestation Requirement

Annually, FDRs must submit an attestation confirming the following:

- Organization has comparable Policies and Procedures and Standards of Conduct that are distributed within 90 Days of hire or contracting, when there are material changes or updates and at least annually thereafter
- Organization complies with the HHS Office of Inspector General (OIG) and the General Services Administration (GSA) System for Award Management (SAM) Exclusion Screening Requirements
- Organization has mechanisms to report suspected or detected issues of non-compliance or FWA
- Organization has established processes to conduct routine monitoring and auditing of downstream and/or related entities to evaluate compliance with applicable laws and regulations

The Plan requests confirmation of compliance thru receipt of the executed FDR Compliance Attestation. Upon the Plan's request, FDRs are required to provide evidence and/or documentation to support compliance with the above requirements.

Tracking and Documenting Compliance Efforts

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

Regularly, the 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 CEO, Compliance Committee, and Board of Directors.

☒ Freedom Health, Inc. ☒ Optimum HealthCare	**Policy Title: Non-Retaliation and Non-Intimidation Policy** **Primary Department: Compliance** **Policy Number: COMP 17** ☒ **Medicare**
Approved By: Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 09/01/2012** | **Effective Date: 09/01/2012** **Revision Date(s): 04/01/2016, 07/20/2017; 04/27/2020** Formerly: COMP 04 (4/1/2012); COMP 22 (3/1/2011)
Reference: 422 CFR 503(b)(4)(vi) and 423 CFR 504(b)(4)(vi); Whistleblower Protection Act of 1989; Florida Whistleblower ACT; Chapter 9 Prescription Drug Benefit Manual and Chapter 21 Medicare Managed Care Manual; The Health Insurance Portability and Accountability Act; Federal False Claims Act; Florida False Claims Act; Title VII of the Civil Rights Act of 1964; Fair Labor Standards Act (FLSA); Family and Medical Leave Act (FMLA); Age Discrimination in Employment Act (ADEA); Americans with Disabilities Act (ADA); Equal Pay Act , and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG")., and COMP 04 Effective Lines of Communication/Disclosure Program.	

POLICY:

The Health Plan is committed to compliance with Federal and State laws and regulations, Program Requirements, the Corporate Integrity Agreement as well as, preventing and detecting any fraud, waste, or abuse. Every director; officer; employee; contractor; first tier, downstream and related entity ("FDR"); consultant and volunteer (collectively referred to herein as "Associates") of the Plan has an obligation to report situations or activities that may violate Federal and/or State laws or regulations, the Plans' policies and procedures and/or Standards of Conduct, and should do so without fear of retaliation or intimidation. The Plan believes every Associate shares a critical responsibility for raising concerns about ethical problems and possible violations of the Plan's policies or the law; therefore, the Plan does not tolerate retaliation or intimidation against any Associate who makes a good-faith report of potential or suspected violations.

In compliance with the Federal and State law and the Corporate Integrity Agreement, the Plan will not permit any intimidation or retaliation against any Associate who raises questions or concerns about misconduct or reports violations of Federal or State laws and regulations, the Plan's policies and procedures, and/or the Standards of Conduct. It is the Plan's policy to comply with all applicable laws that protect Associates against unlawful discrimination, intimidation, or retaliation by their employer or colleagues as a result of their lawfully reporting information regarding actual or potential violations of federal or state law and regulatory requirements by the Plan or its FDRs, or their participating in investigations of any such violations.

PROCEDURE:

The Plan is committed to providing a workplace environment and business relationship conducive to open discussion of its practices to ensure corporate compliance is a culture where Associates feel comfortable in reporting any suspected instances of violations of law or regulations, plan policies, Standards of Conduct, Medicare Program non-compliance or potential FWA. Specifically, this policy prevents any Associate from being subject to adverse action by the Plan or any of its agents as a result of the Associate's act of engaging in a statutorily protected activity, including:

- disclosing information to a government or law enforcement agency, where the Associate has reasonable cause to believe that the information discloses a violation or possible violation of Federal or State law or regulation; or
- reporting suspected violations of Federal or State laws and regulations or Plan policies and/or the Plan's Standards of Conduct; or
- providing information, causing information to be provided, filing, causing to be filed, participating in an investigation or otherwise assisting in an investigation or proceeding regarding any conduct that the Associate reasonably believes involves a compliance violation of any sort; or
- objecting to, or refusing to participate in, any activity, policy, or practice of the employer which is in violation of a law, rule, or regulation

Examples of adverse actions include, but are not limited to:

- Unfavorable employment actions such as termination, demotion, reduction in compensation, suspension, and/or refusal to hire or promote;
- Discrimination and/or harassment;
- Intimidation, humiliation, or social isolation, which can occur directly or indirectly (e.g., via e-mail);
- Creating a hostile and/or intimidating or offensive work environment; and
- Any other actions that are likely to deter an associate from engaging in a protected activity.

Adverse action(s) do not include disciplinary action(s) taken against an Associate as a result of the Associate's own violation(s) of laws or regulations, Plan policies or procedures or negative comments in an otherwise positive or neutral evaluation or negative comments that are justified by an employee's poor work performance or history.

Associates can report suspected violations anonymously, if so desired. Whether reported anonymously or not, the Compliance Department is responsible to keep such information confidential, unless such confidentiality would hinder the investigation.

Associates who file reports or provide evidence which they know to be false or without a reasonable belief the truth and accuracy of such information will not be protected by the above statement and may be subject to disciplinary action, up to and including termination of their employment, agreement or relationship with the Plan.

Except to the extent required by law, the Plan does not intend this policy to protect Associates who violate the confidentiality of any applicable lawyer-client privilege or physician-patient privilege to which the Plan or its agents may be entitled under laws, or to protect Associates who violate their confidentiality obligations with regard to the Plan's trade secret information.

Associates who believe they have been intimidated and/or retaliated against in violation of this policy are encouraged to seek guidance from the Human Resources or Compliance Department. Associates may submit a written or oral complaint, anonymously and confidentially, to the Human Resources or Compliance Department for review and disposition. If it is determined that an Associate has experienced any improper action in violation of this Policy, appropriate corrective action will be taken against the Associate committing any form of a retaliatory act.

Associates concerned about possible acts of intimidation and/or retaliation may also use other reporting methods, anonymously and confidentially, as indicated below:

- **Compliance Hotline:** 1-888-548-0094 (24 Hours a Day/7 Days a week)
- **Compliance Fax:** 1-888-548-0092 (24 Hours a Day/7 Days a week)
- **Compliance Email:** compliancereporting@americas1stchoice.com

  (24 Hours a Day/7 Days a week)
- **Compliance Online Form:** www.americas1stchoice.ethicspoint.com

  (24 Hours a Day/7 Days a week)
- **Compliance Post Office Box:**
  Compliance Reporting,
  P.O. Box 152137, Tampa, FL 33684
  (24 Hours a Day/7 Days a week)

In conjunction with this policy, please refer to COMP 04 Effective Lines of Communication/Disclosure Program for further details on obligations and reporting mechanisms available.

☒ **Freedom Health, Inc.** ☒ **Optimum HealthCare**	**Policy Title: OIG Excluded and GSA Sanctions** **Primary Department: Compliance** **Policy Number: COMP 18** ☒ **Medicare**
Approved By: Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 01/01/2013** **Effective Date: 01/01/2013** **Revision Date(s): 04/12/2016; 07/20/2017; 04/27/2020**
Reference: Medicare Managed Care Manual Chapter 21; Prescription Drug Benefit Manual Chapter 9; The Act §1862(e)(1)(B), 42 CFR §§ 422.503(b)(4)(vi)(F); 422.752(a)(8); 423.504(b)(4)(vi)(F); 423.752(a)(6); 1001.1901; Civil Monetary Penalties Law, 42 USC Section 1320a-7a(a)(5), 42 USC 1395 y(e); 1396a(a)(39), 45 CFR Part 76, , 42 CFR Parts 1000, 1001, 1002 1006 and the Corporate Integrity Agreement (the "CIA") between the Corporation and the Office of Inspector General of the U.S. Department of Health & Human Services (the "OIG").	

POLICY:

Federal law prohibits entities that participate in Federal Health Care Programs, from entering into or maintaining certain relationships with individuals or entities that are ineligible or have been excluded from participation in Federal Health Care Programs and/or have been convicted of a criminal offense that falls under the scope of 42 U.S. Code § 1320a–7a, but has not yet been excluded. Federal funds may not be used to pay for services, equipment or drugs prescribed or provided by a provider, supplier, employee or FDR excluded by the DHHS OIG or GSA.

The purpose of this policy is to set forth the procedures the Health Plan follows in determining whether potential and current Health Plan employees, temporary employees, volunteers, consultants, governing body members and/or first tier downstream related entities are excluded from participation in such federal programs.

The Office of Inspector General (OIG) 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 Federal Health Care Programs. The List of Excluded Individuals/Entities contains just the exclusion actions taken by the OIG. The General Service Administration (GSA) administers the Excluded Parties List System (EPLS) and the System for Award Management (SAM), both of which contain debarment actions taken by various Federal agencies, including exclusion actions taken by the OIG.

In accordance with federal law, the Health Plan has implemented safeguards to identify providers, suppliers, employees, or FDRs excluded by the DHHS OIG and GSA. Prior to engaging in services with employees, temporary employees, volunteers, consultants, governing body members and/or first tier downstream related entities, the Plan requires those to disclose whether they are excluded or ineligible from participation in such federal programs.

The HealthPlan reviews and documents the verification screening of the OIG List of Excluded Individuals/Entities and SAM.gov prior to the hiring or contracting of all prospective employees, temporary employees, volunteers, consultants, governing body members and/or first tier downstream related entities and monthly thereafter to ensure those individuals are not included on such exclusion lists.

The Health Plan will not knowingly employ, contract, engage with, or purchase from individuals or entities that are excluded by the OIG or appear on the GSA's exclusion list. Additionally, the Health Plan will terminate any employment or contract agreement with any individuals or entities that are found to be excluded from participation in federal programs.

Duty to Disclose

All employees, board members, officers, vendors, contractors, first tier downstream related entities responsible for administering or delivering benefits and/or services must immediately disclose if they, or upon discovery, another employee becomes subject to exclusion. Employees, contractors, and/or FDRs who do not comply with this obligation may be subject to disciplinary action, in accordance with the Disciplinary Action policy.

PROCEDURE:

The following screening procedures will be conducted by various Health Plan departments.

Initial Screening

A. New Hire Screening:

1. Prior to employment, HR requires prospective applicants to certify that they are not presently excluded or at risk of exclusion as a result of an existing or recently completed investigation by the State or Federal governments.

2. Prior to the hiring of any Health Plan employee, the Human Resources (HR) Department screens all potential employees by checking the OIG's List of Excluded Individuals/Entities on the OIG web site (http://exclusions.oig.hhs.gov/) and GSA's System for Award Management (www.sam.gov).

B. Credentialing Screening: The Credentialing Department reviews the DHHS OIG List of Excluded Individuals and Entities (LEIE List) and the System for Award Management (SAM.gov) which contains the Excluded Parties List System (EPLS) as part of the Initial Credentialing and Re-Credentialing processes to identify providers and practitioners who have been excluded from participation in Federal Health Care Programs.

C. Sales and Marketing Screening: The Health Plan's Sales and Marketing Department screens all employed agents, contracted downstream independent brokers/agents, and downstream brokers/agents of contracted Field Marketing Office's (FMO's) against the OIG List of Excluded Individuals and Entities (LEIE List) and the System for Award Management (SAM.gov), which contains the Excluded Parties List System (EPLS), who wish to sell Medicare Advantage products on behalf of the Plan.

D. First Tier, Downstream, and Related Entities (FDRs) Screening: The FDR Oversight Team conducts a review of the DHHS OIG List of Excluded Individuals and Entities (LEIE List) and the System for Award Management, which contains the Excluded Parties List System (EPLS), prior to contracting with an FDR.

Monthly Screening

Monthly OIG/GSA screening is essential to prevent inappropriate payment to providers, pharmacies, and other entities that have been added to the exclusions lists since the initial check. After employees, contractors and first tier entities are initially screened against the LEIE and the System for Award Management exclusion databases, the Health Plan conducts a monthly review using the LEIE monthly supplement files provided each month and the monthly Exclusion Extract Data Package Report from SAM.gov.

Monthly screening is conducted by the respective departments below.

A. Human Resources: Conducts monthly screening verification of the exclusion databases to ensure that any employee, temporary employees, contractor, consultant or volunteer responsible for administering or delivering benefits and/or services is not excluded from Federal health care programs.

B. Provider/Practitioner Screening: The Credentialing Department compares the LEIE monthly supplement and monthly Exclusion Extract Data Package Report from SAM.gov to the Health Plan's list of providers/practitioners.

C. Sales and Marketing Screening: The Health Plan's Sales and Marketing Department conducts monthly screening verification of the exclusion databases to ensure that all employed agents, contracted downstream independent brokers/agents, and downstream brokers/agents of contracted

Field Marketing Office's (FMO's) are not excluded from Federal Health Care Programs.

D. **First Tier, Downstream, and Related Entities (FDRs)**: FDR Oversight conducts monthly review of the LEIE supplement files and Exclusion Extract Data Package Report from SAM.gov. to ensure FDRs are not excluded from Federal Health Care Programs.

FDR Oversight also ensures through auditing, monitoring and/or annual attestation process that FDRs are conducting the screening verification of the exclusion databases prior to hiring or contracting and monthly thereafter to ensure that any employee, manager, contractor or volunteer responsible for administering or delivering benefits and/or services is not excluded from Federal Health Care Programs.

The Health Plan requires the immediate removal from any work related directly or indirectly to all Federal Health Care Programs for those whose search yields a verified match to the exclusion lists.

Business Agreements

Legal Counsel will ensure that business agreements include language requiring those to maintain full participation status in the Federal Health Care Programs.

Identification of Excluded Individual/Entity

If the Health Plan identifies or receives actual notice that an individual/entity has become an Ineligible Person, the Health Plan shall remove such individual/entity from responsibility for, or involvement with, the Health Plan's business operations related to the Federal Health Care Program from which such individual/entity has been excluded and shall remove such individual/entity from any position for which the individual/entity's compensation or the items or services furnished, ordered, or prescribed by the individual/entity are paid in whole or part, directly or indirectly, by any Federal Health Care Program from which the individual/entity has been excluded at least until such time as the individual/entity is reinstated into participation in such Federal Health Care Programs.

If the Health Plan has actual notice that an individual/entity is charged with a criminal offense that falls within the scope of 42 U.S.C. §§ 1320a-7(a), 1320a-7(b)(l)-(3), or is proposed for exclusion during the individual/entity 's employment or contract term, the Health Plan shall take all appropriate actions to ensure that the responsibilities of that individual/entity have not and shall not adversely affect the quality of care rendered to any beneficiary or the accuracy of any claims submitted to any Federal Health Care Program.

☒ **Freedom Health, Inc.** ☒ **Optimum HealthCare**	**Policy Title: Anti-Discrimination** **Primary Department: Compliance** **Policy Number: COMP 19** ☒ **Medicare**
Approved By: Diane E.A. Kortsch 04.27.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 08/01/2013** **Effective Date: 08/01/2013** **Revision Date(s): 04/01/2016; 04/19/2017; 04/27/2020** Previously QM23
Reference: Medicare Managed Care Manual Chapter 4, 42 C.F.R. 422 CMS Medicare Prescription Drug Benefit Manual Chapter 5, 42 C.F.R. 423, 45 C.F.R. 90 – 91;	

POLICY:

The Health Plan is committed to adhering to all applicable Federal and State laws and regulations. In order to achieve this goal, the Plan maintains updated policies and procedures regarding beneficiary protections, including protection from discriminatory practices, accomplished by regularly reviewing federal and state laws and regulations.

In addition to State and Federal discrimination laws, the Plan monitors federal laws and regulations; including, but not limited to:

- Civil Rights Act – which prohibits discrimination on the basis of race, color, or national origin
- Age Discrimination Act – which prohibits discrimination on the basis of age;
- Rehabilitation Act of 1973 – which prohibits discrimination on the basis of handicap;
- Americans with Disabilities Act – which prohibits discrimination on the basis of disability and requires reasonable accommodation for persons with disabilities; and
- Genetic Information Nondiscrimination Act of 2008 – which prohibits the use of genetic information in health insurance and employment.
- Section 1557 of the Patient Protection and Affordable Care Act.

The Health Plan complies with requirements for anti-discrimination, including practices related to enrollment, disenrollment, and delivery of health care services by supporting members' rights to receive services without discrimination from the plan and/or plan providers; regardless of race, ethnicity, national origin, pre-existing condition, religion, gender, age, health status, claims experience, medical history, mental or physical disability, sexual orientation, genetic information, evidence of insurability, geographic location within the service area, or source of payment or whether or not an individual has executed an advance directive.

The Health Plan does not target beneficiaries from higher income areas or state or otherwise imply that they are available only to seniors rather than to all Medicare beneficiaries. Only SNPs and MMPs may limit enrollment to dual eligible, institutionalized individuals, or individuals with severe or disabling chronic conditions and/or may target items and services to corresponding categories of beneficiaries. Basic services and information must be made available to individuals with disabilities, upon request. Key areas within the Health Plan, affected by anti-discrimination, also maintain anti-discrimination policies and procedures.

The plan does not deny, limit or condition enrollment to individuals eligible to enroll in a MA plan offered by the organization on the basis of any factor that is related to health status, including but not limited to the following:

- Claims experience;
- Receipt of healthcare;
- Medical history and medical condition including physical and mental illness;
- Genetic information;
- Evidence of insurability, including conditions arising out of acts of domestic violence or;
- disability

PROCEDURE:

1. The Health Plan performs ongoing monitoring to ensure compliance with all applicable regulations, including review of:
    - Provider contracts/agreements
    - Provider manuals
    - Member materials
    - Workforce education and in-service materials
    - Plan policies and procedures
    - Network development
    - Member programs, including medical management, disease management, and/or case management
    - Appeals/Grievances
    - FDR compliance

2. The Plan provides information to members about its anti-discrimination policies through member materials.

The Plan provides information to members about their right to file a complaint with state and federal agencies regarding discrimination at the time of enrollment and annually thereafter.

☒ **Freedom Health, Inc.** ☒ **Optimum HealthCare**	**Policy Title: Disaster and Emergency Declaration** **Primary Department: Compliance** **Policy Number: COMP 20** ☒ **Medicare**
Approved By: Diane E.A. Kortsch 04.28.2020 Diane Kortsch *Date* *Staff VP Compliance*	**Create Date: 11/01/2013** **Effective Date: 11/01/2013** **Revision Date(s): 04/01/2016; 08/30/2017; 04/28/2020**
Reference: Medicare Managed Care Manual Chapter 4, Medicare Prescription Drug Manual Chapter 5, Social Security Act, Stafford Act, National Emergencies Act, and Public Health Service Act	

POLICY:

The Health Plan has established a Disaster and Emergency Declaration policy in accordance with state and federal laws and related regulations.

In the event of a Presidential emergency declaration, a Presidential (major) disaster declaration, a declaration of emergency or disaster by a Governor, or an announcement of a public health emergency by the Secretary of Health and Human Services, but or prior to the issuance of, an 1135 waiver by the Secretary, the Health Plan will:

- Allow Part A/B and supplemental Part C plan benefits to be furnished at specified non-contracted facilities, in accordance with 42 CFR §422.204(b)(3);
- Waive in full, requirements for authorization and pre-notification referrals where applicable;
- Temporarily reduce plan-approved out-of-network cost-sharing amounts to in-network cost sharing amounts.
- Waive the 30-day notification requirement to enrollees as long as all the changes (such as reduction of cost-sharing and waiving authorization) benefit the enrollee; and
- Provide access to Part D drugs dispensed at out-of-network pharmacies when Part D drugs at a network pharmacy cannot be obtained in accordance with Chapter 5 of the Medicare Prescription Drug Manual.
- Allow affected enrollees to obtain the maximum extended day supply, if requested and available at the time of refill.

If, in addition to a Presidential declaration of a disaster or emergency under the Stafford Act or National Emergencies Act, the Secretary of Health and Human Services declares a public health emergency under section 319 of the Public Health Service Act, the Secretary has the right to exercise his or her waiver authority under section 1135 of the Social Security Act. If an 1135 waiver is issued, CMS will identify consequent requirements and responsibilities to the Health Plan.

Under the Secretary's section 1135 waiver authority, CMS may authorize Medicare Administrative Contractors to pay for Part C-covered services furnished to beneficiaries enrolled in the Health Plan and seek reimbursement from the Health Plan for those health care services, retrospectively.

PROCEDURE:

A. In the event of a Presidential major disaster, emergency declaration, or public health emergency the Compliance Department will distribute notification to all business areas.

B. The Compliance Department will monitor the Department of Health and Human Services (DHHS) website (http://www.dhhs.gov) and the CMS website (http://www.cms.hhs.gov) for additional guidance and requirements, including timeframes associated with those requirements during such disasters and emergencies.

C. Plan will disclose policies about providing benefits during disasters on the Plan website.

D. Each business area will ensure appropriate action is taken, in accordance with state and federal laws and related regulations.

E. Access to Part C Provider Network: Typically, the source that declared the disaster will clarify when the disaster or emergency is over. If, however, the disaster or emergency time frame has not been closed 30 days from the initial declaration, and if CMS has not indicated an end date to the disaster or emergency, the Health Plan will resume normal operations 30 days from the initial declaration. If the Health Plan is unable to resume normal operations after 30 days, the Health Plan will notify CMS.

F. Access under Part D: In the event of a Presidential major disaster, emergency declaration, or public health emergency in which the underlying circumstances are reasonably expected to result in a disruption in access to covered Part D drugs, the Health Plan will lift the "refill-too-soon" edits. The Health Plan may exercise some operational discretion as to how these edits are lifted during a disaster or emergency as long as access to Part D drugs is at the point-of-sale. For instance, the Health Plan may implement an edit that is readily resolvable at the point-of-sale through the use of a pharmacist override code.

   The Health Plan will continue to lift edits until the termination of a public health emergency or the end of a declared disaster or emergency.

- In the case of a public health emergency, it terminates when it no longer exists or upon the expiration of the 90-day period beginning from the initial declaration, whichever occurs first.

- For major disasters declared by the President, the Health Plan will monitor FEMA's website, for the closure of disaster incident periods listed in the Disaster Federal Register Notice section (http://www.fema.gov/news/disasters.fema). In circumstances in which the incident period has not officially closed 30 days from the initial Presidential declaration, the Health Plan may consider extending the implementation of the edits but is not required to do so. If the Health Plan chooses to remove the edits, the Health Plan will work closely with enrollees who indicate that they are still displaced or otherwise impacted by the disaster or emergency.

In the absence of a Presidential major disaster or emergency declaration or a public health emergency, the Health Plan may consider lifting the edits, for instance, in advance of an impending disaster; if the Health Plan determines it appropriate to do so to ensure pharmacy access.

The Health Plan will ensure that enrollees have adequate access to covered Part D drugs dispensed at out-of-network pharmacies during any Federal disaster declaration or other public health emergency declaration in which enrollees are evacuated or otherwise displaced from their place of residence and cannot reasonably be expected to obtain covered Part D drugs at a network pharmacy.

Affected enrollees will be allowed to obtain the maximum extended day supply, if requested and available at the time of refill.