MEDICARE & HIX COMPLIANCE DEPARTMENT
COMPLIANCE & FRAUD, WASTE AND ABUSE PROGRAM

January 1, 2018

Dear Meridian Family Members and Contractors:

At Meridian Health Plan, we have a corporate responsibility of providing industry-leading health services at low cost to the people and communities we serve in. We also hold ourselves to the highest ethical standards by following the rules and regulations that govern our business.

This Compliance and Fraud Waste and Abuse (FWA) Program ("Compliance Program") is fully supported by our Executive Leadership and endorsed by the Board of Directors. Our Compliance Program is the cultural and operational foundation from which we run our business and adhere to State and Federal laws, regulations and our internal policies and procedures.

At Meridian, we believe that compliance is everyone's responsibility and each one of us has the authority and duty to do the right thing. We thank you for your continued support in our ongoing commitment to serve our members in the best and most ethical manner.

TABLE OF CONTENTS

MEET OUR COMPLIANCE DEPARTMENT

Our Medicare Compliance Department is made up of healthcare professionals with years of experience in the compliance, healthcare and Medicare field. Our team comprises of processionals in the areas of audit, healthcare administration, legal, and science and medicine.

MEET OUR COMPLIANCE LIAISONS

The Compliance Liaison Program establishes compliance ambassadors within operational areas. The liaisons serve to ensure that compliance best practices are proactively embedded into the daily operations of the company. Acknowledging that compliance is every employee's responsibility and not just those individuals with formal compliance roles, we recognize that there is a business need to adopt a best practice and place compliance personnel in strategic locations within high-risk operational areas to maximize compliance effectiveness.

LINES OF BUSINESS

This Compliance and FWA Program applies to Meridian's Medicare and Health Insurance Exchange (HIX) line of business. Unless otherwise stated, the requirements contained herein shall apply to both lines of business.

WHO DOES THIS APPLY TO?

This Compliance and FWA Program applies to all Meridian Health Plan employees, officers, Board and Committee members, and first tier, downstream or related (FDR) entities that contract with Meridian Health Plan to perform a core Medicare and Health Insurance Exchanges (HIX) service (hereafter "covered person(s)").

WHAT ARE MY EXPECTATIONS?

You are required to read and be familiar with this Compliance and FWA Program at the time of your hire, appointment or contracting, and annually thereafter. You should learn to recognize potential noncompliant and FWA issues that may arise during your work, report them to the appropriate channel, and assist in remediating them. You should strive to improve your department's process to minimize compliance risks to Meridian Health Plan, our members, and our State and Federal regulatory agencies. Ultimately, you can be a champion and an advocate for compliance, and be a part of our culture of compliance.

DISSEMINATION

This Compliance and FWA Program is disseminated in accordance to the following schedule:

At time of hire: Human Resources shall disseminate the Compliance and FWA Program, including the Code of Business Conduct and Ethics, to employees within **90 days** of hire. Employees shall sign an acknowledgment of receipt.

Annually: Human Resources shall disseminate the Compliance and FWA Program, including the Code of Business Conduct and Ethics, to employees **annually** thereafter, and when there are substantial updates.

FDR: The contract administrator shall disseminate the Compliance and FWA Program and Code of Business Conduct and Ethics to applicable FDRs within **90 days** of contracting, using Appendix II of the Pre-Delegation Compliance Checklist posted on our website. The Compliance Department disseminates the document to the FDRs **annually** thereafter. Meridian Health Plan may use various dissemination methods, including:

- Hard copies
- Electronic copies
- Posting on company intranet

The respective disseminating party shall document that this has been done, including any record of acknowledgment of receipt, and provide evidence to the Compliance Department for retention.

OUR COMPLIANCE PROGRAM AT A GLANCE

The Compliance Program and the content contained herein are a collection of incorporated policies, procedures, and guidance by which our Medicare and HIX program are governed. These policies implement the Compliance and FWA Program. The FWA Plan and Code of Business Conduct and Ethics are also incorporated within the Compliance Program. If an applicable policy exists outside of the Compliance Program, it will be referenced accordingly.

The Compliance and FWA Program consists of 7 core elements. Each core element has its own policy and procedure that implement that particular element. For your convenience, here is a summary of each element:

Element 1 (Compliance with State and Federal Laws): We must comply with applicable laws and regulations that pertain to Medicare and HIX, such as HIPAA, Federal False Claims Act, and the Social Security Act.

Element 2 (Compliance Officer and Compliance Committee): We must maintain a Medicare & HIX Compliance Officer and a Compliance Committee to oversee the enforcement and effectiveness of the Compliance and FWA Program.

Element 3 (Compliance Training): We must administer effective training and education for all employees, Board and Committee members, and applicable FDRs at the time of hire, appointment or contracting, and annually thereafter.

Element 4 (Effective Lines of Communication): We maintain effective lines of communication to ensure that you can report compliance and FWA issues to the appropriate channel, including anonymous and confidential reporting.

Element 5 (Disciplinary Standards): In order to be effective, we must maintain disciplinary standards to ensure that people who commit a compliance or FWA violation are subject to appropriate corrective actions, up to and including termination of employment or contract.

Element 6 (Monitoring and Auditing): We adopt the doctrine of "trust but verify". We conduct routine monitoring reviews and audits of our internal operations and external business partners to ensure that they are performing in accordance with State and Federal guidelines.

Element 7 (Compliance Investigation & Corrective Action Plan): Lastly, upon discovery of a potential noncompliant or FWA issue, we will initiate a thorough investigation of the incident. We then track deficiencies and instances of noncompliance by formal Corrective Action Plans (CAP) to ensure that they are remedied and are not likely to reoccur.

COMPLIANCE POLICIES

POLICY NUMBER C-1: COMPLIANCE WITH FEDERAL & STATE LAWS

POLICY

Meridian Health Plan will comply with applicable Federal and State laws and statutes, Code of Federal Regulations, and sub-regulatory guidance.

PROCEDURE

Meridian Health Plan administers its compliance program in accordance with the following statutes, laws, regulations, and agency requirements that are promulgated by the Federal and State government. Applicable covered persons are required to maintain current knowledge of these requirements, and implement and integrate the requirements within the operational, administrative and compliance areas.

Anti-Kickback Statute: This statute prohibits anyone from knowingly and willfully receiving or paying anything of value to influence the referral of federal health care program business, including Medicare and Medicaid. This can take many forms, such as cash payments, entertainment, credits, gifts, free goods or services, the forgiveness of debt, or the sale or purchase of items at a price that is not consistent with fair market value. It also may include the routine waiver of co-payments and/or co-insurance.

The offense is classified as a felony and is punishable by fines of up to $25,000, imprisonment for up to five years, civil money penalties up to $50,000, and exclusion from participation in federal health care programs.

Anti-Money Laundering: Money laundering involves hiding the origin of unlawfully gained money, for example through drug transactions, bribery, terrorism or fraud. Meridian Health Plan is committed to complying fully with all anti-money laundering laws and regulations. We will conduct business only with reputable customers involved in legitimate business activities, with funds derived from legitimate sources.

Antitrust Laws: These laws are designed to protect competition by prohibiting monopolies, price fixing, predatory pricing and other practices that restrain trade. We never discuss pricing, suppliers or territories with competitors, nor make agreements with them on these or other competitive issues. We gain information about competitors only in legal and ethical ways. Competitor proprietary information that is improperly obtained cannot be used to the advantage of Meridian Health Plan.

Beneficiaries Inducement Statute: Medicare marketing guidelines prohibit Meridian Health Plan from offering rebates or other cash inducements of any sort to beneficiaries. The guidelines prohibit us from offering or giving remuneration to induce the referral of a Medicare beneficiary, or to induce a person to purchase, or arrange for, or recommend the purchase or ordering of an item or service paid in whole or in part by the Medicare program.

Civil Monetary Penalties: In addition to criminal penalties, the United States Government may also impose civil monetary penalties and exclude a person or entity from participation in Medicare and all other Federal health care programs.

Code of Federal Regulations: Meridian Health Plan must comply with Federal regulations that implement and oversee the Medicare and HIX program. These regulations include:

42 CFR §400: Overview

42 CFR §403: Special programs
42 CFR §411: Benefit and payment exclusions
42 CFR §417: Health maintenance organizations, competitive medical plans, and health care prepayment plans
42 CFR §422: Medicare Advantage program. This is the authoritative regulation that implements the Medicare Advantage Program under the Social Security Act
42 CFR §423: Prescription drug program. This is the authoritative regulation that implements the Prescription Drug Program under the Social Security Act
42 CFR §430: Medicaid program. This is the authoritative regulation that implements the Medicaid Program under the Social Security Act
42 CFR §1001: OIG program exclusions
42 CFR §1003: OIG civil money penalties, assessments and exclusions
45 CFR §144-159: This is the authoritative regulation that implements HIX
29 CFR §2560: Department of Labor regulations that govern aspects of HIX

Contractual Commitments: Meridian Health Plan contracts with government agencies such as the Centers for Medicare and Medicaid Services (CMS), the Michigan Department of Community Health (MDCH) and the Illinois Department of Healthcare and Family Services (HFS) to administer the Medicare Advantage (MA) and Medicare-Medicaid Plan (MMP) program. We are bound by the terms and conditions of those contracts. Non-compliance with contractual obligations may result in the suspension or termination of our contracts with CMS and the State.

Federal Criminal False Claims Statutes: Federal laws make it a criminal offense for anyone who makes a claim to the United States government knowing that it is false, fictitious, or fraudulent. This offense carries a criminal penalty of 5 years in prison and a monetary fine.

False Claims Act: This act prohibits any person from engaging in any of the following activities:

1. Knowingly submit a false or fraudulent claim for payment to the United States Government;
2. Knowingly make a false record or statement to get a false or fraudulent claim paid or approved by the Government;
3. Conspire to defraud the Government by getting a false or fraudulent claim paid or approved by the Government; or
4. Knowingly make a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the Government.

Violations may result in a civil penalty of not less than $5,000 and not more than $10,000, plus 3 times the amount of damages which the Government sustained due to the violation.

The False Claims Act (FCA) defines "knowingly" broadly to mean a person who: (1) has actual knowledge of the information; (2) acts in deliberate ignorance of the truth or falsity of the information; or (3) acts in reckless disregard of the truth or falsity of the information, even without a specific intent to defraud.

The FCA also allows an individual to file a *qui tam* action that entitles the individual to receive between 15-30 % of a settlement or action stemming from the suit. Under the FCA, individuals are protected from being discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in their employment as a result of filing a *qui tam* action. Remedies include reinstatement with the same seniority, two times the amount of any back pay, interest on any back pay, and compensation for any

special damages sustained as a result of the discrimination, including litigation costs and reasonable attorneys' fees.

Federal Food, Drug and Cosmetic Act: This Act authorizes the FDA to oversee drugs and medical devices.

Fraud Enforcement and Recovery Act of 2009 (FERA): This law reinforces criminal violations of certain federal fraud laws, federal false claim laws, including financial institution fraud, mortgage fraud, and securities and commodities fraud.

Health Insurance Portability and Accountability Act (HIPAA) & HITECH Act: These acts protect the confidentiality and integrity of protected health information. The HIPAA Privacy Rule provides federal protections for personal health information held by Meridian Health Plan and its business partners and gives patients an array of rights with respect to that information.

The Security Rule specifies a series of administrative, physical, and technical safeguards for Meridian Health Plan and its business partners to use to assure the confidentiality, integrity, and availability of electronic protected health information.

OIG List of Excluded Individuals and Entities (LEIE) & GSA System for Award Management (SAM): Federal law prohibits the payment by Medicare, Medicaid or any other federal health care program for any item or service furnished by a person or entity excluded from participation in these federal programs. No Part C or D Sponsor or FDR may submit for payment any item or service provided by an excluded person or entity, or at the medical direction or on the prescription of a physician or other authorized person who is excluded. The Office of Inspector General (OIG) maintains the LEIE and the General Services Administration (GSA) maintains the SAM.

Patient Protection and Affordable Care Act: This law requires health insurers to sell insurance to individuals regardless of their health status or any pre-existing medical conditions, requires individuals who don't have health insurance to purchase health insurance or face a penalty, and created a health insurance exchange system that allows individuals to purchase standardized, State-regulated health care plans that are eligible for federal subsidies.

Physician Self-Referral ("Stark") Statute: This statute, which is also articulated in §1877 of the Social Security Act, prohibits a physician from making referrals for certain designated health services (DHS) payable by Medicare to an entity with which he or she (or an immediate family member) has a financial relationship (ownership, investment, or compensation), unless an exception applies. The statute prohibits the submission of claims to Medicare for those referred services.

Record Retention: CMS requires that we maintain for a period of **10 years** all applicable documents and evidence related to ownership and operation of our financial, medical, and other record keeping systems, financial statements, Federal income tax or returns, asset acquisition, lease or sale agreements, contracts, and subcontracts (including franchise, marketing, and management agreements), claim charges and payment, costs of operations, income received by source and payment, cash flow statements, and any financial reports filed with Federal programs or State authorities.

Social Security Act: Title XVIII of the Social Security Act implements the Medicare Advantage Program (§1851-1859) and the Prescription Drug Program (§1860D-1860D-31), and serves as the statutory foundation by which these two Medicare programs are governed. In addition, and when applicable,

Meridian Health Plan complies with Original Medicare requirements under §1811-1848. Title XIX of the Social Security Act implements the Medicaid program (§1900-1946).

Sub-Regulatory Guidance: CMS issues sub-regulatory guidance such as HPMS memos, manuals, instructions, and memos. Meridian Health Plan shall comply with such guidance.

REFERENCES

- Chapter 9: Prescription Drug Benefit Manual-Compliance Program Guidelines (§50.1)

POLICY NUMBER C-2: COMPLIANCE OFFICER, COMPLIANCE COMMITTEE & GOVERNING BODY

POLICY

Meridian Health Plan maintains a Medicare & HIX Compliance Officer and a Medicare & HIX Compliance Committee. The Compliance Officer and Compliance Committee are accountable to members of the Executive Leadership, and report to the Board of Directors and CEO on the activities and status of the Compliance Program at least quarterly.

The Compliance Officer is vested with the day-to-day operations of the compliance program, is an employee of the organization, and reports to a member of Executive Leadership. In no event shall the Compliance Officer be an employee of Meridian Health Plan's first tier, downstream and related entity (FDR), or serve dual roles in operational areas.

The Compliance Committee advises the Compliance Officer, and assists in the implementation of the Compliance Program. The Board of Directors is accountable for and exercises reasonable oversight over the effectiveness and implementation of the Compliance Program, and maintains current knowledge about the content and operation of the Compliance Program.

PROCEDURE

COMPLIANCE OFFICER

Reporting & Accountability: The Medicare & HIX Compliance Officer reports to and is directly accountable to the Executive Vice President and General Counsel, a member of the organization's Executive Leadership.

The Compliance Officer reports *at least quarterly* to the Compliance Committee and Board of Directors on the activities and status of the Compliance Program, including issues identified, investigated, and resolved by the Compliance Program. This is done to ensure that committee members, senior management, and Board members are knowledgeable about the content and operation of the compliance program, and that they exercise reasonable oversight with respect to the implementation and effectiveness of the compliance program. The Compliance Officer has the authority to provide unfiltered, in-person reports to the Board of Directors.

The Compliance Officer also provides quarterly compliance reports to the CEO of Meridian Health Plan, either directly or through the Executive Vice President and General Counsel. However, the Compliance Officer has the authority to provide unfiltered, in-person reports to the CEO of Meridian Health Plan.

Roles & Responsibilities: The Compliance Officer maintains the following, but not limited, roles and responsibilities:

1. Implement the Compliance Program, including defining the program structure, educational requirements, reporting and complaint mechanisms, response and correction procedures, and compliance expectations of all personnel and FDRs.

2. Provide compliance reports *at least quarterly* to the Board of Directors, CEO and Compliance Committee on the status of the Compliance Program, the identification and resolution of potential or actual instances of noncompliance, and the compliance oversight and audit activities.

3. Interact with business owners and operational units and being involved in and aware of the daily business activities. The Compliance Officer implements this by engaging in operational meetings.

4. Create and coordinate (or delegate) educational training programs to ensure that officers, directors, managers, employees, FDRs, and other individuals working in the Medicare and HIX program are knowledgeable about the Compliance Program, written Code of Business Conduct and Ethics, compliance policies and procedures, and all applicable statutory and regulatory requirements.

5. Develop and implement methods and programs that encourage managers and employees to report program noncompliance and suspected FWA and other misconduct without fear of retaliation.

6. Maintain the compliance reporting mechanism and closely coordinate with the internal audit department, where applicable.

7. Respond to reports of potential instances of FWA, coordinate internal investigations and develop appropriate corrective or disciplinary actions, if necessary.

8. Coordinate personnel issues with Human Resources to ensure that covered persons are checked against the OIG exclusion lists and GSA debarment lists monthly. Meridian Health Plan may require the FDRs to provide signed attestation/certification of their compliance with this requirement, subject to validation.

9. Maintain documentation for each report of potential noncompliance or FWA received from any source, which describes the initial report of noncompliance, the investigation, the results of the investigation, and all corrective and/or disciplinary action(s) taken as a result of the investigation.

10. Oversee the development and monitoring of corrective action plans.

11. Coordinate potential fraud investigations/referrals with the appropriate National Benefit Integrity Medicare Drug Integrity Contractor (NBI MEDIC), collaborate with other sponsors, State Medicaid programs, Medicaid Fraud Control Units (MFCUs), commercial payers, and other organizations, where appropriate, when an FWA issue is discovered that involves multiple parties.

12. Has the authority to:
    - Interview employees regarding compliance issues.
    - Review and retain company contracts and other documents.
    - Review the submission of data to CMS and State agencies to ensure accuracy and compliance with CMS and State reporting requirements.
    - Seek independent advice from legal counsel.
    - Report misconduct to CMS or law enforcement.
    - Conduct and direct internal audits and investigations of any FDRs.
    - Recommend policy, procedure and process changes.

Training & Maintaining Current Knowledge: The Compliance Officer maintains current and comprehensive knowledge of Federal and State regulations and program requirements through various methods, including reading HPMS memos, manuals, attending industry-sponsored conferences, and interacting with other plans' compliance officers.

In addition, the Compliance Officer participates (or delegates) in important government-sponsored conferences and workgroups such as:

- Spring/Fall CMS Medicare Advantage and Prescription Drug Plan Conference
- CMS-sponsored Center for Program Integrity (CPI) NBI MEDIC Fraud Work Group Quarterly Meetings
- Monthly Issues Management with CMS Regional Officer

COMPLIANCE COMMITTEE

Purpose: The Compliance Committee is responsible for advising the Compliance Officer and assisting in the implementation and administration of the Compliance Program. The Committee oversees compliance for the Medicare and HIX line of business.

Reporting & Accountability: The Compliance Committee is accountable to the Chief Administrative Officer. Through the Compliance Officer, the Compliance Committee reports at least quarterly to the Board of Directors on the status and effectiveness of the Compliance Program.

Membership[1]: The Compliance Committee maintains memberships from a variety of backgrounds, including Pharmacy Services, Health Services, Legal, Human Resources, Operations, IT, Business Development and representatives from the Executive Leadership. Committee members have decision-making authority in their respective business area of expertise.

Membership considerations, including the addition and removal of committee members, can be made by any committee member at any time. An assessment of the adequacy of the current membership representation shall be conducted on an annual basis.

Meeting Protocol: The committee shall meet at least quarterly. Meetings shall be documented by minutes. Relevant documentations submitted to the committee shall be retained in accordance with CMS record retention requirements.

Roles & Responsibilities: The Committee maintains the following, but not limited, roles and responsibilities:

1. Meet at least quarterly.

2. Develop strategies to promote compliance and the detection of potential violations.

3. Review and approve compliance and FWA training, and ensure that training and education are effective and appropriately completed.

[1] Membership listing may be modified from time to time without requiring Compliance Committee approval of updates to this policy.

4. Assist with the creation and implementation of risk assessment and monitoring and auditing work plan.

5. Assist in the creation, implementation and monitoring of effective corrective actions.

6. Develop innovative ways to implement appropriate corrective and preventative action.

7. Review the effectiveness of the system of internal controls designed to ensure compliance with regulations in daily operations.

8. Support the Compliance Officer's needs for sufficient staff and resources to carry out his/her duties.

9. Ensure up-to-date compliance policies and procedures.

10. Ensure that there is a system for employees and FDRs to ask compliance questions and report potential instances of noncompliance and FWA confidentially or anonymously without fear of retaliation.

11. Review and address reports of monitoring and auditing of areas at risk for noncompliance or FWA and ensure that corrective action plans are implemented and monitored for effectiveness.

12. Provide regular and ad hoc reports on the status of compliance with recommendations to the governing body.

BOARD OF DIRECTORS/GOVERNING BODY

The Board of Directors exercises reasonable oversight in the development and implementation of the Compliance Program, and is ultimately accountable for compliance. On an annual basis, the Board shall adopt a resolution stating the organization's commitment to lawful and ethical conduct. The Board also approves the Code of Business Conduct and Ethics. This function may not be delegated.

The Board acts as a policy-making body that exercises oversight and control over policies and personnel to ensure that management actions are in the best interest of the organization and its enrollees. The policy-making body also controls the appointment and removal of the Medicare executive manager.

The Board maintains the following, but not limited, roles and responsibilities:

1. Understand the compliance program structure.

2. Be informed about compliance enforcement activities such as notices of non-compliance, warning letters, and other formal sanctions.

3. Be informed of compliance program outcomes, including results from internal and external audits.

4. Receive regularly scheduled updates, measurable evidence, and data from the Compliance Officer and Compliance Committee showing that the compliance program is detecting and correcting noncompliant issues on a timely basis.

5. Review results from the assessment of the Compliance Program's performance and effectiveness.

6. Be knowledgeable about the content and operation of the compliance program through updates, training and education on the structure and operation of the Compliance Program.

In addition, Board members stay engaged in the oversight of the compliance program by continually asking critical questions, such as:

- What does the Board need to do to stay educated on new regulations?
- Where are the compliance risk areas?
- What operational areas are performing well and not performing well, and what is the root of success and lack of success?
- What areas are strong and weak within the compliance program, and what is the root to the strength and weakness?
- What are the primary root causes to compliance issues?
- Do the reports given to the Board provide the appropriate level of detail that the Board needs to oversee the program?
- Is the compliance program effective and how does the Compliance Department measure compliance effectiveness?
- How does the Compliance Department ensure that the work it is doing appropriately addresses the risks associated?
- What is the Compliance Officer's escalation process when dealing with difficult issues, such as repeat findings and issues that management may not be responsive to resolve?
- Does the Compliance Officer have the freedom and authority to provide unfiltered reports to the Board without fear of retaliation?
- Does management support the compliance program?
- What is management doing to ensure CAPs are resolved timely, and repeat findings do not occur again?
- What is management doing to hold people accountable for non-performance?
- What types of internal controls are in place (as instituted by management) to ensure processes are running in a compliant manner?
- Are departments adequately staffed and trained to achieve success?
- What is the company doing to prevent issues from occurring?
- What is the company doing to ensure compliance improvement from year-to-year?
- How is the company performing relative to CMS expectations, the competitors, and the industry as a whole?

CEO & Executive Leadership Engagement

The CEO of Meridian Health Plan and applicable Executive Leadership shall ensure that the Compliance Officer is integrated into the organization and is given the credibility, authority and resources necessary to operate a robust and effective compliance program. The CEO receives periodic reports from the Compliance Officer on risk areas facing the organization, the strategies implemented to address those risks, and the results of those strategies. The CEO is advised of all governmental compliance enforcement activity, including Notices of Non-Compliance and formal enforcement actions.

REFERENCES

- 42 CFR §422.503(b)(4)
- Chapter 9: Prescription Drug Benefit Manual-Compliance Program Guidelines (§50.2)

POLICY NUMBER C-3: COMPLIANCE TRAINING & EDUCATION

POLICY

Meridian Health Plan administers effective training and education for all covered persons who are responsible for the administration or delivery of a Medicare and HIX program at the time of hire or contracting, and annually thereafter. Training and education cover general compliance training, specialized compliance training, and fraud, waste and abuse (FWA) training.

PROCEDURE

RESPONSIBILITY

Compliance Department: Creates general and FWA training content for all covered persons; administers training to Board of Directors, and committee members (including the Pharmacy and Therapeutics (P & T) Committee and Compliance Committee); creates the Specialized Training Checklist for high-risk departments; administers ad-hoc specialized training to high-risk departments; posts compliance posters in high-visible common areas; distributes the annual training to FDRs and disseminates compliance tips to raise compliance awareness.

Human Resource: Administers general and FWA training to employees; maintains records of time, attendance and results of training.

Sales Department: Creates (or delegates) agent/broker training content and administers (or delegates) training for agents and brokers; maintains records of time, attendance and results of training.

Operational Departments: Create and administer specialized training for their employees; administer initial training to FDRs (or ensure that FDRs complete their own training); maintain records of time, attendance and results of training.

FDRs: Create and administer the training for their employees; maintain records of time, attendance and results of training; submit attestation/certification of their compliance with this requirement, subject to validation of compliance.

Provider Network: Administers compliance training to contracted providers.

GENERAL & FWA COMPLIANCE TRAINING

Meridian Health Plan administers effective general and FWA training and education to covered persons who are responsible for the administration or delivery of the Medicare and HIX program benefit in accordance with the following schedule:

Employees: Within **90 days** of hire, and annually thereafter as a condition of employment.

Board and Committee Members: Within **90 days** of appointment, and annually thereafter.

FDRs: Within **90 days** of contracting, and annually thereafter. The only acceptable training modules are those:

- Developed by Meridian Health Plan (using CMS-approved modules);
- Developed by another Medicare Advantage plan (using CMS-approved modules); or
- Developed by CMS through its Medicare Learning Network (MLN) website https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Fraud-Waste_Abuse-Training_12_13_11.pdf. Effective 2016, this will be the only acceptable option.

The FDR may develop its own modules to provide employees with specific, on-the-job training. It may also develop additional training to supplement the General Compliance and FWA Training content, but it cannot replace them. Meridian Health Plan may require the FDRs to provide signed attestation/certification of their compliance with this requirement, subject to validation of compliance. Meridian Health Plan may also validate the FDR's compliance with this requirement through auditing a sample of the highest risk FDRs.

Agents/Brokers: During the initial and annual sales appointment process. In no event may an agent or broker be appointed or market to a beneficiary without completing training.

Providers: Within **90 days** of contracting, and annually thereafter. Providers who have met the FWA certification requirements through enrollment into the Medicare program or accreditation as a Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) are deemed to have met the training and educational requirements for fraud, waste, and abuse. However, these providers still must receive general compliance training.

Pharmacies: For network pharmacies, we require the pharmacy benefits manager (PBM) to administer the training to its network pharmacies.

All records of time, attendance and results of employee training will be documented in the LMS system. FDRs are responsible for tracking and maintaining training records. All training records must be retained for a minimum period of **10 years**. Compliance training materials are updated annually, and contain topics such as:

- Description of the Compliance Program, including a review of compliance policies and procedures, the Code of Business Conduct and Ethics, and the organization's commitment to business ethics and compliance with all government program requirements.
- How to ask compliance questions, request compliance clarification or report potential noncompliance, emphasize confidentiality, anonymity, and non-retaliation for compliance related questions or reports of potential noncompliance or FWA.
- Requirement to report potential compliance and FWA issues.
- Examples of reportable compliance and FWA issues.
- Disciplinary guidelines for non-compliant or fraudulent behavior, communicate how such behavior can result in mandatory retraining and may result in disciplinary action, including possible termination when such behavior is serious or repeated or when knowledge of a possible violation is not reported.
- Attendance and participation in formal training programs as a condition of continued employment and a criterion to be included in employee evaluations.
- Policies related to contracting with the government, such as the laws addressing fraud and abuse or gifts and gratuities for government employees.
- Potential conflicts of interest and the disclosure requirement.

- HIPAA, the CMS Data Use Agreement, and the importance of maintaining the confidentiality of personal health information.
- Monitoring and auditing process and work plan.
- Laws that govern employees and the compliance program.
- Laws and regulations related to FWA (i.e. False Claims Act, Anti-Kickback statute, HIPAA).
- Obligations of FDRs to have appropriate policies and procedures to address FWA.
- Process for reporting suspected FWA.
- Protections for those who report suspected FWA.
- Types of FWA that can occur in the settings in which employees work.

SPECIALIZED COMPLIANCE TRAINING

Meridian Health Plan requires covered persons to receive specialized training and education based on their specific responsibilities in high risk government business areas in accordance with the following schedule:

Employees: Within **90 days** of hire, and annually thereafter (as needed) as a condition of employment. This includes employees who change job functions within the organization.

FDRs: Within **90** days of contracting, and annually thereafter as needed). Meridian Health Plan may require the FDRs to administer its own training, and provide signed attestation/certification of their compliance with this requirement, subject to validation of compliance.

All records of time, attendance and results of training will be documented by the respective departments responsible for administering the training. Specialized training topics in high risk areas include, but are not limited to:

- Sales and marketing
- CDAG
- ODAG
- Formulary administration
- Compliance program
- Bid
- Provider Network
- Call center
- Claims
- Enrollment and disenrollment
- Health services
- Premium billing

Please refer to the individual department for a detailed listing of require specialized training content. On an as-needed, the Compliance Department will conduct training in specific departments covering high risk topics. In addition, the Compliance Department will provide ongoing training to the Compliance Committee, Board of Directors and Executive Leadership through formal training, regulatory updates, industry best practices, and information obtained from government agency and industry conferences and workgroups.

MEMBER, FDR & AD-HOC TRAINING

The Compliance Department routinely conducts ad-hoc in-class trainings in certain high-risk departments. We also provide ongoing training and education to our members and FDRs.

MEASURE OF EFFECTIVENESS

Training effectiveness is measured by a number of methods, including:

- Number of CAPs
- Results from compliance audits
- Requests for compliance interpretation
- CMS self-disclosure
- Training follow-up assessment
- Decrease in compliance issues or findings in a business area
- Increase in compliance awareness
- Increase in compliance inquiry and reporting

REFERENCES

- Chapter 9: Prescription Drug Benefit Manual-Compliance Program Guidelines (§50.3)

POLICY NUMBER C-4: EFFECTIVE LINES OF COMPLIANCE COMMUNICATION, REPORTING & NON-RETALIATION

POLICY

EFFECTIVE LINES OF COMMUNICATION

Meridian Health Plan maintains effective lines of communication to ensure confidentiality between the Compliance Officer, Compliance Committee, employees, managers and Boards of Directors, and first tier, downstream and related entities (FDRs). The lines of communication are accessible to all, allow compliance issues to be reported when they arise and provide a means for anonymous and confidential good faith reporting of potential compliance issues as they are identified.

REPORTING

In order to ensure ethical conduct, all covered persons have an obligation to raise concerns they might have about conduct that falls short of compliance standards, and report issues to the appropriate channel. They are also expected to assist in the investigation and resolution of compliance and fraud, waste or abuse (FWA) issues. Failure to do so may result in disciplinary actions, up to and including termination of employment or contract.

NON-RETALIATION

To create a work environment where employees and individuals feel comfortable addressing and reporting any instances of non-compliance or FWA, unfair or unethical acts, Meridian Health Plan maintains a non-intimidation and non-retaliation environment that allows individuals to make good faith reports against any person or action by Meridian Health Plan or its FDRs, without repercussion or fear of retaliation. Those who retaliate against an individual who makes a good faith effort to report a compliance or FWA issue will be subject to corrective action.

PROCEDURE

COMPLIANCE COMMUNICATION

The Compliance Officer routinely communicates compliance and FWA requirements throughout applicable areas of the organization using various channels, such as email, internet website, and other methods.

The Compliance Department disseminates updated regulatory guidance and instructions, including CMS HPMS memorandums, manuals, and the Part C/D User Group Calls to applicable business departments. We track and document this process to ensure that new regulations and instructions are properly implemented. Business owners are responsible for taking follow-up actions to ensure compliance with the new requirements. Areas of deficiency must be communicated to the Compliance Department immediately. The regulatory dissemination process is as follows:

HPMS Notices:

1. Upon receipt of an HPMS memo or other State and Federal guidance, the Compliance Department logs the document in the HPMS Notice Tracking Module and assigns them to business owners

within **1-2 business days** of receipt. If the memo is urgent or time sensitive, we will forward the memo via email to the business owner for immediate action.

2. Memos are classified based on:
    a. **RISK:**
        i. **High:** This designation is reserved for memos that are of the highest risk based on a Compliance assessment of high complexity, implementation challenges, impact to members, impact to a CMS program audit area, level of business burden and current status of operational readiness.
        ii. **Medium:** This designation is used for most memos and reflects moderate complexity, implementation challenges, impact to members, impact to a CMS program audit area, level of business burden and current status of operational readiness.
        iii. **Low:** This designation is used for some memos and reflects low complexity, implementation challenges, impact to members, impact to a CMS program audit area, level of business burden and current status of operational readiness.
    b. **FOLLOW-UP LEVEL:**
        i. **No Follow-Up:** The memo is low-medium risk and no Compliance follow-up is needed.
        ii. **Follow-Up Needed:** The memo is high risk and requires Compliance to conduct **at least 1** follow-up within a **30-day period** (or earlier or later if the memo warrants) with business owners on the current status of implementation.

    While each memo will be assessed against these parameters, the parameters are independent of each other and Compliance reserves the right to take actions that are commensurate with the memo, rather than apply a linear approach. For example, a memo may be **High Risk**, but may be deemed **No Follow-Up**.
3. For high-risk memos and guidance that have significant operational impact, significant changes to current processes, or cross-functional impact, the Compliance Department will analyze them for content and applicability, meet with individual business owners to discuss their action plan, and answer any interpretation questions. Important memos are also discussed during the bi-monthly Government Operations meeting as a standing agenda item. Notes taken during these meetings are incorporated into the HPMS memo as part of the HPMS Notice Tracking Module.
4. Each business owner receives an immediate email notification from SharePoint indicating that a memo has been assigned to them.
5. The business owners will have **7 business days** (**14 business days** for complex guidance) to review the guidance and document the action plan in the HPMS Notice Tracking Module. The actual action or implementation plan may take longer to develop, but the initial analysis and response must occur within **7/14 business days**.
6. Once all necessary actions have been taken, the business owner will mark the action task as "Complete" which will notify Compliance. Prior to closing out the case, Compliance reviews each response to ensure appropriate and complete actions have been/will be taken.
7. If the business owner's comments are incomplete, we will work with the business owner to ensure all appropriate actions are taken and documented properly in SharePoint.
8. Compliance will conduct follow-up outreach for memos marked as **Follow-Up Needed**.
9. Non-responses will follow the escalation procedure:
    a. SharePoint will send a reminder **1 day** before the upcoming deadline [this will be a manual process until we deploy the automated SharePoint solution]

b. SharePoint will send a reminder **1 day** past the deadline [this will be a manual process until we deploy the automated SharePoint solution]

Departments showing a pattern of non-responsiveness or untimeliness will receive further compliance remedial action, up to and including a CAP.

10. The Compliance Department will incorporate high-risk requirements from the guidance into existing auditing and monitoring protocols to verify the accurate and timely implementation of the requirements.
11. On a **bi-weekly** basis, Compliance will review all outstanding notices to ensure appropriate and complete actions have been taken.
12. The Compliance Department will participate in operational meetings to provide oversight of complex or high-risk issues. Business owners are also encouraged to request the Compliance Department participate in other operational meetings during implementation.

The business owners (who receive direct notices from HPMS) should not wait for the Compliance Department to send out the HPMS dissemination email. Rather, they should start the process of reviewing and analyzing the memos right away and take the appropriate actions necessary to meet the memo's content.

Part C/D User Group Calls: The Compliance Department also tracks and documents regulatory guidance through the CMS user group calls, and communicates this to business owners when applicable. Compliance sends out notices to business owners impacted by the content of the call. We retain documentation of the calls, including recorded audit, in SharePoint.

CMS Educational Notices: The Compliance Department routinely disseminates new compliance information to business owners and applicable FDRs. The notices summarize changes in CMS regulations, CMS sanctions and enforcement actions against other health plans, CMS conferences, and industry/association training and conferences.

Employee Newsletter: We provide compliance newsletters as an additional line of communication between our employees and the Compliance Officer and Compliance Department, with tips and instructions on how to detect and report FWA. The newsletters also provide information on disciplinary standards and non-retaliation and non-intimidation policy.

Compliance Posters: We routinely disseminate compliance posters, tips, and FAQs and post them in highly visible common areas to raise awareness of compliance requirements, FWA implications, non-retaliation, and reporting protocols.

Regulatory Interpretations: You can request clarification on a regulatory or compliance question, or request an interpretation of the rule by contacting the Compliance Officer directly or any member of the Compliance Department.

MEMBER & FDR COMMUNICATION

The Compliance Department, in collaboration with operational partners, communicates compliance and FWA requirements to beneficiaries and existing members through various methods, including member website, marketing materials, and member newsletters.

In addition, Meridian Health Plan maintains a Compliance Website accessible to FDRs and members that contain information on FWA training and reporting.

REPORTING REQUIREMENT

All covered persons must report a compliance or FWA issue within **7 calendar days** of discovering the potential violation. Examples of issues that must be reported include:

- CDAG and ODAG
  - Untimely effectuation
  - Inappropriate denials
  - Access to care issues
  - Member notice issues
  - Misclassification of cases
- Untimely or inaccurate EOB
- Call center
  - Not meeting performance standards
  - Inaccurate information provided
  - Downtime
- Enrollment & disenrollment
  - Untimely member notice
  - Inappropriate enrollment & disenrollment
- Premium billing
  - Untimely or inaccurate billing
  - Invoice issues
- Formulary administration
  - Access to care issues
  - Inappropriate denials
  - Untimely transition claims
  - Protected class drug issues
- Issues caused by an FDR
- Sales and marketing
  - Untimely or inaccurate ANOC/EOC
  - Inappropriate agent/broker behavior
- Claim
  - Access to care issues
  - Untimely or inaccurate claim adjudication
  - Inappropriate denial of benefits
- Provider network
  - Access issues
  - Credentialing issues
- HR
  - Excluded persons
- IT issues that trigger deficiency in any of the above-referenced areas

METHOD OF REPORTING

Meridian Health Plan maintains various lines of communication to ensure confidentiality in reporting. The communication channels are accessible to all. Any covered person may report a compliance or FWA issue, concern, or violation through the following methods:

1. Report to your immediate supervisor.
2. Report directly to your Meridian contract administrator
3. Report to the Meridian Compliance Officer
4. Report anonymously to EthicsPoint 24 hours a day/7 days a week
   http://mhplan.ethicspoint.com/
   1-855-375-6725

If you are a Meridian Health Plan vendor, in addition to any of the methods outlined above, you may report to your Meridian Health Plan contract administrator.

REPORTING PROTOCOLS

When reporting, please be sure to provide enough information about the situation to allow us to investigate it, such as:

- Your name and contact information (optional)
- Description of the incident
- Business area(s) involved
- Names of individuals involved
- Date when event or incident occurred
- Whether this is a one-time incident or reoccurring event

The Compliance Department, Human Resources, or the appropriate department investigating the incident will document all reports of a compliance or FWA issue, concern, or violation, and shall initiate an investigation within **2 weeks** of receiving the report. When appropriate and possible, you will be provided a response on the outcome of the investigation. Please refer to the *Policy Number C-7: Compliance Investigations* for a detailed description of the investigative process.

NON-RETALIATION

No employees will be discriminated or retaliated against in any way for bringing forward a question or good faith complaint. All employees are required to support both the letter and spirit of this commitment. Those who retaliate against an individual who makes a good faith effort to report a compliance or FWA issue will be subject to Meridian Health Plan's corrective action policy.

Furthermore, if you are filing a *qui tam* action under the Federal False Claims Act, you are protected by law from being discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in your employment as a result of filing a *qui tam* action.

If you suspect that you are being retaliated against for making a good faith report of a compliance or FWA issue, you may contact any person(s) outlined in this policy, including the Compliance Officer or a member of Human Resources.

Your allegation of retaliation will be investigated by the appropriate personnel, and those who are found to have violated Meridian Health Plan's non-retaliation Policy will be subject to the disciplinary policy.

DISCLOSURE TO CMS

In the spirit of transparency, the Compliance Department may disclose to the CMS Regional Office applicable incidents of noncompliance and FWA that impact beneficiary safety and access to care. We will provide the Regional Office with regular updates on the status and outcome of corrective action plans and any follow-up monitoring activities that may be done to ensure that the issue is not likely to reoccur.

COORDINATION WITH HUMAN RESOURCES

For issues that have an impact on personnel matters, Human Resources will be engaged appropriately to handle compliance or FWA issues that impact such personnel matters.

EXIT INTERVIEW

Employees who depart from Meridian Health Plan's employ are given an Exit Interview Questionnaire, which asks the departing employee to evaluate the effectiveness and availability of the organization's line of communications to report compliance and FWA concerns. Human Resources will review each Exit Interview Questionnaire for compliance reporting, and inform the Compliance Department appropriately.

DOCUMENTATION & INVESTIGATION

The Compliance Department will document and retain all reports of compliance and FWA issues in their original content. Please see the *Policy Number C-7: Compliance Investigations* for a detailed description of the investigative process.

REFERENCES

- Chapter 9: Prescription Drug Benefit Manual-Compliance Program Guidelines (§50.1.5, 50.1.7)

POLICY NUMBER C-5: PERSONNEL CORRECTIVE ACTIONS

POLICY

Meridian employees must comply with all governing laws and regulations, provisions of our compliance program, Code of Conduct, Employee Handbook, HIPAA Privacy and Security regulations and all other applicable company policies in the performance of job duties. Performance issues often affect Meridian and its affiliated health plans' ability to meet contractual, statutory and other obligations. Meridian's policy with respect to administering corrective actions is designed to ensure that employees whose performance or conduct does not meet the company's standards are treated fairly and in a consistent manner. Employees whose performance or conduct does not meet the Company's standards will be subject to corrective actions based on the severity of the issue up to and including dismissal and risk potential reporting to law enforcement/regulatory agencies.

While this policy encompasses our intended range of disciplinary standards and procedure, nothing in this or any other policy shall be construed to preempt, delay or otherwise limit our ability to take appropriate action, up to and including immediate termination, in any circumstance that Meridian, in its sole discretion, deems necessary. Nothing in this policy shall modify the at-will nature of employment nor create any expectation of any employment contract or policy other than at-will as set forth in Meridian's employment policies, procedures and manuals. These procedures do not create any contractual obligation on the part of Meridian. The procedures are provided as a guideline for discipline in those situations where the company, in its sole discretion, believes that such action is in the best interest of both the company and the employee.

PROCEDURE

SITUATIONS WHICH DISCIPLINARY ACTION IS NECESSARY

The below lists are not exhaustive of all types of conduct that may constitute grounds for disciplinary action and whether an item is listed has no bearing on whether an issue may result in discipline. Employees should always use their best judgment to determine whether a course of action complies with the mission, values and culture of the company. Examples of the types of performance or compliance infractions or violations or workplace issues for which discipline or corrective action will be taken include:

1. Noncompliance with laws, regulations, payor contracts, policies or procedures;
2. Encouraging or assisting another to engage in noncompliance;
3. Failure to report known noncompliance;
4. Failure to detect noncompliance by an individual who should have detected such noncompliance;
5. Knowingly submitting a false, malicious or frivolous report of noncompliance against another employee. No employee shall be disciplined solely because he or she reported what was reasonably believed to be an act of wrongdoing or a violation of the Compliance Program.
6. Failure to satisfy the education and training requirements of the Compliance Program;
7. Failure of a supervisor or manager to assure that their subordinates understand the requirements of the Program;
8. Retaliation or intimidation against an Employee, Agent, or Contractor who reports in good faith a concern relating to possible noncompliance; or

9. Violation of Privacy and Security policies and procedures.
10. Performance failures or attitude issues not related to compliance such as:
    a. Insubordination;
    b. Neglect of duty, or any failure on the part of any employee to perform any part of his or her job duties or assigned tasks;
    c. Attendance or tardiness issues; or
    d. Actions taken during at company sponsored events, on company property, or in performance of duties that do not meet company values.

HIPAA NON-COMPLIANCE

HIPAA noncompliance produces varying level of risk for the company. Generally, noncompliance falls into the following categories:

1. **Level I Offense**: Improper and/or unintentional disclosure of PHI or records.
    a. This level of offense occurs when an employee unintentionally or carelessly accesses, reviews or reveals consumer or employee PHI to himself or others without a legitimate need-to-know.
    b. First time offenses in this category generally result in a documented verbal warning with additional education.
2. **Level II Offense**: Unauthorized use and/or misuse of PHI or records.
    a. This level of offense occurs when an employee intentionally accesses or discloses PHI in a manner that is inconsistent with MHP policies and procedures, but for reasons unrelated to personal gain.
    b. First time offenses in this category generally result in a written warning combined with additional education and a PIP however an egregious Level II Offense will likely result in a final written warning.
3. **Level III Offense**: Willful and/or intentional disclosure of PHI or records.
    a. This level of offense occurs when an employee accesses, reviews or discloses PHI for personal gain or with malicious intent.
    b. Any offense in this category will generally result in immediate termination and may result in referral to law enforcement as deemed appropriate.

NON-COMPLIANCE

Noncompliance can take many forms and often overlaps with performance deficiencies. Examples of noncompliance may include:

- **Bid**: Overstating or understating bid data to obtain higher premiums from members or higher reimbursement from the government.
- **Call center**: Providing beneficiaries with inaccurate information.
- **Claims**: Submitting claims to the government for services that were never rendered, failure to pay providers at the correct rate, paying providers who are on the Medicare opt-out or OIG exclusion list.
- **Enrollment and disenrollment**: Improperly enrolling members to obtain higher reimbursement from the government, improperly disenrolling members due to high medical expenses or other medically-related reasons.
- **Exceptions and appeals**: Not approving members for medically necessary services.
- **Health services**: Failing to approve members for medically necessary services.

- **Premium billing**: Billing members at the incorrect premium amount, not providing members with the required grace period to pay their bills.
- **Pharmacy**: Denying members their transition supply, applying utilization management rules that have not been approved, inappropriately denying drugs that should be covered.
- **Provider network**: Not credentialing providers in accordance with credentialing laws and regulations, contracting with providers who are on the Medicare opt-out or OIG exclusion list.
- **Sales and marketing**: Misleading beneficiaries, violating a CMS marketing rule, allowing agents and brokers to conduct illegal marketing activities.

INVESTIGATION

A thorough investigation must be conducted before disciplinary action is administered. Depending on the situation, the investigation may be conducted by the supervisor, manager, Human Resources, Compliance Department, Legal Department or an outside entity. All employees are required to assist in the resolution of the investigation in the appropriate manner. Employees who willfully hinder the investigation will themselves be subject to disciplinary action.

APPROPRIATE DEGREE OF PROGRESSIVE DISCIPLINE

Evaluation of Relevant Circumstances:

Leadership must consider the nature and seriousness of the infraction, all relevant facts and information, and any mitigating or aggravating circumstances when formulating disciplinary action. All guidelines must be applied consistently and in a non-discriminatory manner, and thorough documentation is essential. Senior leadership, the Compliance Department, Human Resources, or the Legal Department should be consulted as appropriate when evaluating the circumstances affecting disciplinary action.

Admission of wrongdoing does not guarantee release from disciplinary or corrective action. The weight to be given to the admission shall depend on all the facts known to Meridian at the time the decision concerning disciplinary or corrective action is made. Such facts include whether the individual's conduct was known or its discovery was imminent prior to the admission, and whether the admission was complete and truthful.

Progressive Steps for Discipline:

The appropriate degree of progressive discipline or corrective action for a particular issue depends on the nature and severity of the infraction, the results of leadership's investigation of the situation, and the evaluation of relevant aggravating or mitigating circumstances. Not all performance or compliance issues lend themselves to the progressive steps listed below. Any disciplinary actions may be taken without regard to prior problems or prior discipline. Certain situations may warrant immediate and serious disciplinary action, including suspension or dismissal.

At each level of progressive discipline, the Employee, his or her supervisor, and a Human Resources representative, as necessary, shall meet to outline the problem(s) and state the supervisor and the Company's expectations.

1. **Documented Verbal Warning:** This is issued for minor infractions and to employees who may not have any prior history of problems.
    a. This meeting is a time to clarify any misunderstood directions, eliminate incorrect assumptions, and resolve any conflicts.

b. The supervisor shall write a summary of the issue outlining the planned corrective action and documenting the meeting for retention in the employee's personnel file.
c. All individuals present at meeting will be required to acknowledge the document in the HR System.

2. **Written warning:** This is issued for moderate to severe infractions, either for the first time or due to the employee's failure to correct the behavior after the Verbal Warning. The employee may also have a history of problems.
    a. This meeting is a time to further clarify any misunderstood directions, eliminate incorrect assumptions, and resolve any conflicts.
    b. The supervisor shall write a summary of the issue outlining the planned corrective action and documenting the meeting for retention in the employee's personnel file.
    c. All individuals present at meeting will be required to acknowledge the document in the HR System.
    d. Employee will be presented with a hard copy of the written warning.

3. **Final written warning:** This is issued when the behavior has not been corrected at the Written Warning level.
    a. A written detail of the problem will be presented with a history of the previous attempts to rectify the problem, e.g. verbal and/or written warnings. Notice will be given to the employee at this time that this is a final warning and immediate corrective action is required.
    b. The supervisor shall write a summary of the issue outlining the planned corrective action and documenting the meeting for retention in the employee's personnel file.
    c. Employee shall be given a hard copy of the final written warning for his or her records.
    d. All individuals present at meeting will be required to acknowledge the document in the HR System.
    e. At HR's discretion, employee may be suspended for one or more days without pay.

4. **Termination:** This is done for serious and egregious infractions, or when the behavior has not been corrected at the Final Written Warning level.
    a. After a verbal warning, written warnings, and suspension, termination for repeated or continued infractions may be called for.
    b. The department supervisor and HR should document a written statement summarizing the reasons for termination in the employee's personnel file.
    c. Any employee receiving a Final Written Warning for the second time over the course of their employment may be immediately terminated.

POLICY CONSISTENCY

Meridian ensures that corrective action policies and actions are applied consistently by:

- Addressing and responding to all inappropriate behavior and poor performance promptly.
- Following the organization's Personnel Corrective Actions Policy when determining that corrective action is appropriate.
- Treating all similar offenses in the same manner while taking into consideration the seriousness of the offense, the consistency with previous corrective actions for similar offenses, any mitigating circumstances, and the offender's prior conduct, past performance record, length of service, and willingness and ability to correct the problem.

OBLIGATION TO REPORT

Meridian requires all employees to report and disclose any potential compliance, HIPAA or FWA issues. Employees are also expected to assist in the investigation and resolution of these issues. Failure to report a compliance issue may result in corrective actions, up to and including termination of employment or contract.

Please refer to our policy on Effective Lines of Compliance Communication, Escalation of Issues, and Enforcement of Well-Publicized Disciplinary Guidelines policies for detail on reporting requirements.

TIMEFRAMES FOR INVESTIGATION AND RECORD RETENTION

Every single performance or conduct issue varies by fact, circumstance, complexity, and resource availability. Thus, it is sometimes not possible to come to a resolution to a performance or compliance issue within a strict and defined timeframe because doing so will compromise the integrity, quality and thoroughness of the issue, specifically if an investigation into the conduct is required. To that end, performance or conduct issues are generally resolved within **30 days** of occurrence. We reserve the right to extend this timeframe for more complex performance or conduct issues.

All disciplinary records must be retained for **10 years**, and capture the dates of the violation, the investigation, the findings, the disciplinary action taken, and the date it was taken.

PROGRESS REPORTS

For performance and compliance issues where HR or the supervisor deems it necessary to revisit the issue, a progress review date will be given. Whether a progress report is necessary will be indicated on the documentation submitted to the employee file. A progress report will be completed by the Director or Manager on the date listed and will be presented to the employee stating whether or not they met the expectations. A representative from the Human Resources Department must be present for the progress report follow-up meeting.

COORDINATION WITH COMPLIANCE

When an individual is subject to corrective action, Human Resources will review the case for compliance violations to ensure that issues impacting compliance are resolved appropriately in addition to the personnel issue. The Compliance Department will be notified of a compliance issue for further compliance action, and inclusion in compliance tracking metrics as applicable.

PUBLICIZING CORRECTIVE ACTION STANDARDS

We publicize corrective action guidelines through various mediums, including during initial employee orientation, at annual compliance training, and in compliance posters and public bulletins. In addition, employees and supervisors are encouraged to discuss corrective action guidelines during regular staff meetings.

PERIODIC COMPLIANCE REVIEW

At least annually, the Compliance Committee shall review this policy with Human Resources and records of discipline applied during the preceding year. The purpose of the review will be to determine whether disciplinary actions were: a) appropriate to the seriousness of the violation, b) fairly and consistently

administered and c) imposed within a reasonable timeframe. If necessary the Compliance Committee shall make changes to this policy or the discipline procedure, including providing additional education to directors, managers and supervisors to ensure proper administration.

REFERENCES

- Chapter 9: Prescription Drug Benefit Manual-Compliance Program Guidelines (§50.5)

POLICY NUMBER C-6: COMPLIANCE MONITORING & AUDITING

POLICY

Meridian Health Plan maintains an effective system for routine monitoring and auditing of operational areas to evaluate the organization's compliance with regulatory requirements and the overall effectiveness of the Compliance Program.

PROCEDURE

COMPLIANCE WORKPLAN

Annually, the Compliance Department conducts a risk assessment of operational areas and develops a workplan. The workplan contains, among others, monitoring and auditing activities to be conducted for that year. The Compliance Department oversees and executes ongoing monitoring and auditing activities in high risk areas, and oversees corrective actions and implementation plans pursuant to a compliance finding.

RISK ASSESSMENT

As a precursor to creating the annual compliance workplan, the Compliance Department conducts a formal risk assessment of compliance and operational issues based on the following, but not limited, criteria:

- CMS audit scope
- CMS areas of concern (i.e., marketing, enrollment, agent/broker oversight, credentialing, quality assessment, appeals and grievance, benefit/formulary administration, transition, protected classes, utilization management, claims processing accuracy, and FDR oversight)
- CMS Common Conditions, Improvement Strategies, and Best Practices
- CMS conferences
- CMS Call Letter
- CMS audit guide
- CMS Enforcement Letters
- CMS Corrective Action Plans
- CMS Regional Office feedback
- HPMS memos
- Impact to beneficiary access to care, safety and protection
- New/updated guidance and regulation
- OIG Workplan
- Results from prior monitoring & auditing activities
- Assessment of all operational areas
- Business owner feedback
- Past compliance issues
- Internal CAPs
- Complaint Tracking Module (CTM)
- Extent of FDR delegated activities
- Industry conferences

- Company/department size, resources, structure, business model
- Complexity of work

Relative to monitoring of FDRs, if it is impractical or cost prohibitive to monitor all FDRs, we will perform a risk assessment to identify the highest risk FDRs, and select a reasonable number of FDRs for review. We will also assess the need to conduct an onsite review versus desktop. High-risk FDRs may undergo an onsite review.

We then conduct interviews with business owners and Executive Leadership to assess their areas of concern, and incorporate those areas into the workplan when appropriate. We then rank the areas by risk, in accordance with the following methodology:

RISK RATING	VALUE	EXPLANATION
3	**High**	The issue has high or significant compliance impact, and is a regular government focus. The issue has a direct member or financial impact and affects beneficiary protection and access to care. Plans have been fined, sanctioned or terminated due to deficiencies due to these issues. It is a mandate to review the majority of high-risk issues. It is a strong recommendation to review the rest of the high-risk issues. Inactivity may lead to significant risk.
2	**Medium**	The issue has medium or moderate compliance impact. The issue has slight financial or member impact. It is recommended that it be reviewed. Inactivity may lead to moderate risk.
1	**Low**	The issue has low compliance impact. It has either been reviewed previously, or is not a focus of the government. Inactivity does not pose a significant or moderate risk.

The compliance workplan is then submitted to the Medicare & HIX Compliance Committee for approval, and reported to the Board of Directors. While the workplan reflects our best effort to assess risks to the organization and mitigate those risks, we recognize that operational and compliance risks and the regulatory landscape are constantly changing. To that end, the workplan is routinely reviewed and revised from time to time to meet those changing needs.

MONITORING REVIEWS

The Compliance Department conducts routine monitoring reviews that measure operational performance in key, high risk areas. Routine monitoring reviews are regular reviews performed as part of normal operations to confirm ongoing compliance and to ensure that corrective actions are undertaken and effective. They follow the following protocols:

1. Each month, the Compliance staff extracts metrics and data from internal systems, business owners, and populated CMS audit universe templates.

2. The data is analyzed and calculated based on CMS requirements, and populated in the Routine Automated Monitoring Reviews Report.

3. Deficiencies and any downward trends (from the previous reporting months) are shared with business owners for correction. If there is a continued pattern of deficiencies, Compliance will initiate a CAP.

4. Compliance may validate the accuracy of the data through ad-hoc sample testing and during our Compliance Audits.

COMPLIANCE AUDITS

The Compliance Department also conducts audits that require an analysis of policies and procedures, interviews with key stakeholders, universe requests, sample extractions, detailed data analysis, extrapolation and testing based on internal and CMS methodologies. Compliance audits are formal reviews of policies and procedures and operational performance against laws and regulations.

All monitoring reviews and audits are conducted in accordance with regulations and requirements and are measured by performance scorecards. When deficiencies are detected pursuant to a monitoring review or audit, follow-up reviews may be conducted to measure the effectiveness of any corrective action. Services of independent external auditors may be retained to assist in the auditing of high-risk areas, including FDRs performing a high-risk function. Compliance audits follow the following protocols:

Phase I: Work Assignment

1. The Compliance Officer will provide business owners with at least 2-4 weeks advance notice before going into an area, with a cc to the FDR if applicable. For a review that impacts an FDR, the FDR will be provided at least 30 days advance notice of the review, or within a timeframe stipulated in the FDR contract.

2. The Compliance Officer assigns an audit to the Compliance Manager and rolls out the audit workbook. The Compliance Manager then assigns a Review Team and Audit Lead to conduct the review. The Review Team is made up of staff personnel from the Compliance Department. Independent contracted auditors may be used to assist the Review Team when necessary. Workbooks are available to Federal and State regulatory agencies upon request.

3. The role of the Compliance Manager and Audit Lead is to:
    a. Manage and coordinate the end-to-end phases of the project.
    b. Develop strategies, in conjunction with the Review Team, to execute the project in an accurate and efficient manner.
    c. Assign work to members of the Review Team in a fair and efficient manner.
    d. Be aware and knowledgeable of all work performed by other members of the Review Team.
    e. Ensure that all work is completed timely and accurately by the Review Team.
    f. Scrutinize the work of the Review Team to meet a satisfactory level of acceptance.
    g. Be the point of contact for the Compliance Officer to receive status updates.

Phase II: Research & Strategy

4. The Review Team:
    a. Reviews the workbook in detail in order to command an expert knowledge of the workbook and all the pertinent regulations contained therein.

b. Develops and formulates review strategies, including methods of critique and scrutiny.
c. Identifies all relevant business owners as accurately and completely as possible.
d. Develops document requests and deadlines.
e. Develops all other project documents prior to meeting with business owners.

Phase III: Entrance Meeting

5. The Review Team schedules an Entrance Meeting with the manager/director of the business unit to go over the following:
    a. Scope of the review
    b. Ownership
    c. Document request
    d. Project deadlines
    e. Business owner's preferred method to deal with FDRs:
        i. (Preferred Method) Review Team works directly with the FDR and keeps the business owner in the loop, or
        ii. Review Team works through the business owner
    f. Business owner's preferred method to provide requested documents, policies and procedures, universes, and samples:
        i. Business owner provides the data/document to the Review Team, or
        ii. Review Team gets access to the system and pulls the data/document itself
    g. Criteria for a Pass, Pass with Observation, Fail, and Recommendation
    h. CAP process, including:
        i. Types of findings that would require a CAP
        ii. CAP timeframe
        iii. CAP tracking and closure process

Phase IV: Review Protocol

6. The Review Team conducts the review.

7. Depending on the scope, universes will be pulled and a sample of typically 30 cases will be selected. The individual audit workbook will stipulate the exact number of samples to be pulled, depending on the risk, scope and resource. For monthly mini-audits, a sample of 5-10 cases are typically pulled.

8. To avoid scope creep, the review should not deviate from the workbook unless out-of-scope issues are discovered that pose significant risk to the member or the organization.

9. The Review Team should resolve business owner delays, delinquencies or pushback, and escalate to the Compliance Manager and Compliance Officer when necessary. Anticipated delays that will jeopardize the review deadline must be communicated to the Compliance Manager and Compliance Officer as soon as possible.

10. The Review Team provides bi-weekly updates (or a greater frequency if needed) to the Compliance Manager and Compliance Officer on the status of the review, issues detected, and risks and concerns.

11. Document all positive and negative findings, including reason for findings, working papers, policies and procedures reviewed, universes and case samples, and any other supporting documentation in a centralized location located in the Compliance Department's SharePoint webpage.

Phase V: Findings

12. The Review Team conducts the review and keeps business owners informed of tentative findings throughout the review.

13. Business owners are given an opportunity to correct findings before our published findings if the findings do not impact issues that would require validation.

14. The following scoring methodology will be applied during an audit:

    a. **Sample Case Accuracy:** A requirement/element will either receive a Pass or Fail, depending on the root cause and number of sample case failures.

       Pass: When the total sample cases yield 80% or greater in compliance, regardless of reason.
       Fail (CAR): When the total sample cases are between 60-79% in compliance, regardless of reason.
       Fail (ICAR): When the total sample cases are below 60% in compliance, regardless of reason. An ICAR will also be assessed for serious issues, regardless of percent of compliance.

       Typical reasons that result in a Fail may include:

       i. Process error or deficiency
       ii. Systemic error or deficiency
       iii. Manual error that is repeated, preventable, and reflects a weak internal process

    b. *Observations*: These are noted for immaterial instances of non-compliance due to isolated human error, universe inaccuracy, and other non-systemic issues. Observations do not require a formal CAP.

    c. *Recommendations*: The requirement/element under review meets the regulatory standards. Compliance is making a recommendation to enhance it based on best practice standard.

15. For audit elements that are covered by a **CMS program audit** scope, the following will be applied:

    a. **Sample Case Accuracy:** See instructions above.
    b. **Universe Timeliness & Performance:** The applicable universe metric will be analyzed for compliance performance based on the following thresholds:
       i. **Pass:** When the universe metric compliance rate is 95% or higher.
       ii. **Fail (CAR):** When the universe metric compliance rate is between 90-94%.
       iii. **Fail (ICAR):** When the universe metric compliance rate is lower than 90%.

c. **Universe Accuracy:** The samples pulled for testing will be compared against data in the universe (to validate the accuracy of the samples and the universe metric) based on the following thresholds:
    i. **Pass:** When the accuracy rate is 95% or higher.
    ii. **Fail (CAR):** When the accuracy rate is between 90-94%.
    iii. **Fail (ICAR):** When the accuracy rate is lower than 90%.

    Universe Performance and Universe Accuracy issues stemming from audit areas not covered by a CMS performance audit scope will be noted as an Observation.

d. One (1) point will be assigned to a corrective action required (CAR) and 2 points will be assigned to an immediate corrective action required (ICAR) for each finding or condition, depending on severity. An audit element will receive multiple points if it fails in Sample Case Accuracy, Universe Performance, and Universe Accuracy. To calculate a Compliance Score, the total points will be divided by the total number of elements/requirements tested:

$$\text{Compliance Score} = \frac{\text{Total number of points}}{\text{Total number of elements or requirement}}$$

    The Compliance Score reflects an operational area's performance relative to the review. A lower score reflects stronger compliance performance compared to a higher score. The Compliance Scores are then classified and defined within the following parameters[2]:

    i. Excellent: Less than 0.4 score
    ii. Good: 0.5-0.9 score
    iii. Average: 1-1.4 score
    iv. Poor: 1.5-2.4 score
    v. Unacceptable: 2.5-higher score

Phase VI: Status Update

16. Close to the review ECD, the Compliance Officer meets with the Compliance Manager and Review Team to go over tentative findings. During the meeting, the Compliance Manager and Review Team must be prepared to:
    a. Discuss all positive and negative findings in detail
    b. Provide rationale, justification and logic to support findings
    c. Provide recommendation and conclusion of findings
    d. Articulate all findings in a clear, concise, and complete manner

Phase VII: Publication

17. The Compliance Manager and Review Team draft a Compliance Audit Report and send to the Compliance Officer for review. By the time the Compliance Officer receives the first draft, the

[2] These internal parameters are established based on industry performance among various health plans, as audited and determined by CMS. Because industry performance may change, the policy and parameters may change from year-to-year.

Compliance Manager/Review Team has already ensured that business owners are aware of the findings, and whenever possible, agree with the findings and recommendations.

18. Upon review of the draft report by the Compliance Officer, the Compliance Manager/Review Team sends the draft report to business owners for review.

19. The Compliance Manager/Review Team disseminates the final report to:
    a. Business owners
    b. The VP executive over the business unit
    c. The Medicare & HIX Compliance Officer

Phase VIII: Corrective Action Plan

20. All deficiencies and findings pursuant to a monitoring review will require a corrective action plan (CAP).

21. All deficiencies and findings, especially those that have a member impact, will be assessed to determine whether they need to be disclosed to Federal and State regulatory agencies in accordance with the agency's reporting and disclosure protocols.

22. We may conduct follow-up reviews to validate that the CAP has been remediated satisfactorily.

REPORTING

All monitoring and auditing activities are reported to the Compliance Committee. The Board of Directors and CEO will receive applicable reports that are relevant and high-risk. Results are also reported via compliance scorecards and other forms of compliance reporting measures.

MEASURING COMPLIANCE EFFECTIVENESS

The overall effectiveness of the Compliance Program is measured by the use of performance dashboards, scorecards, metrics reporting, and other similar measures. We measure program effectiveness by parameters such as:

- Results and trends from comprehensive monitoring reviews (i.e., number of Pass and Fail)
- Results and trends from routine monitoring reviews and quantitative measurement tools in high-risk areas such as agent/broker oversight, compliance program effectiveness, enrollment and disenrollment, Part C ODAG, Part D CDAG and Part D formulary administration
- Annual Compliance Program Effectiveness Assessment
- Number of CAPs opened
- Effectiveness of CAP in resolving issues
- Number of reoccurring CAPs impacting the same issue
- FDR compliance
- CMS notices of non-compliance, warning letters and sanctions
- Marketing material approval rates
- Number of detected or self-reported issues
- Number of issues disclosed to CMS

- Number of disciplinary actions
- Trend analysis over a monthly, quarterly, semi-annual, or annual period
- Compliance training completion and test score results
- Trend in CTM cases
- Self-assessments and surveys

The effectiveness of the Compliance Program is evaluated frequently, at least annually. The results are reported to Compliance Committee, Board of Directors and CEO.

AUDIT WORKPLAN

As part of developing the annual work plans, the Compliance Department and Internal Audit will coordinate their activities and work plans to ensure that high-risk areas are adequately covered, and that the work plans are administered in a timely and efficient manner throughout the year.

As part of this coordination, the Compliance Department and Internal Audit will share monitoring review results and audit findings and other areas of concerns in order to adequately address those issues.

Please refer to the Internal Audit Plan for a detailed description of the Internal Audit Department's auditing principles and protocols.

ANNUAL COMPLIANCE PROGRAM ASSESSMENT

On an annual basis, Meridian Health Plan shall audit the effectiveness of the compliance program through the use of third-party independent auditors or Internal Audit personnel who are not a part of the Compliance Department. The results shall be reported to the Medicare & HIX Compliance Committee, Boards of Directors and CEO.

REFERENCES

- Chapter 9: Prescription Drug Benefit Manual-Compliance Program Guidelines (§50.6)

POLICY NUMBER C-6A: EXCLUSION & BACKGROUND CHECK

POLICY

Meridian Health Plan shall not hire, contract with, or allow any individual who has been sanctioned or excluded from participating in Medicare, Medicaid or HIX programs to work in such programs.

All new and existing employees, board members and officers, and contractors are to immediately disclose to Meridian Health Plan any debarment, exclusion or any other event that makes them ineligible to perform work related directly or indirectly to Federal health care programs.

In addition, Meridian Health Plan will conduct other background checks prior to an offer of employment, such as criminal records, driving records, and education and professional credentials.

Meridian Health Plan will not contract with or pay claims to providers who have been sanctioned or excluded from participating in Medicare, Medicaid or HIX programs, or who have opted-out of the Medicare program.

All contracted providers are to immediately disclose to Meridian Health Plan any debarment, exclusion or any other event that makes them ineligible to perform work or receive payment for work related directly or indirectly to Federal health care programs.

PROCEDURE

EXCLUSION LIST

The OIG's List of Excluded Individuals/Entities (LEIE) and GSA's System for Award Management (SAM) search utilizes the government's database for individuals and businesses excluded or sanctioned from participating in Medicare, Medicaid HIX or other federally funded programs. Basis for exclusions include convictions for program-related fraud and patient abuse, licensing board actions, and default on Health Education Assistance loans. Any applicant, board member or officer appearing on this list will not be considered for employment or appointment.

At Time of Hire/Appointment:

Step 1: Prior to any offer of employment or appointment, a member of HR will check the OIG LEIE and GSA SAM for all candidates, board members and officers.

Step 2: The LEIE search is performed via an internet database, http://exclusions.oig.hhs.gov/. The SAM search is performed via https://www.sam.gov/portal/SAM/#1. The search is conducted using the first and last name of the applicant. The results are then printed and retained in the individual's confidential personnel file.

- *Match*: If a search of the database results in a match with a name in the database, verify the identity of the individual by entering the social security number.

    - Before taking adverse action, HR will provide the applicant a pre-adverse action disclosure that includes a copy of the LEIE match, and a copy of "A Summary of Your Rights Under the Fair Credit Reporting Act."

- Once the decision is made not to hire the applicant, HR will provide the applicant notice that the action has been taken in an adverse action notice.

- *No Match*: If a search of the database results in no name matches, the message will state no record found and the individual's confidential reference file will reflect this.

Monthly Review:

Step 1: Each month, HR will check the LEIE and SAM for all employees, Board members and officers to ensure that no existing individuals are on the list.

- *Match*: If any individual is on such list, Meridian Health Plan shall require the immediate removal of such individual from any work related directly or indirectly to all Federal health care programs, and may take appropriate corrective actions, up to and including termination of employment or contract.

- *No Match*: The individual's confidential reference file will reflect this.

OTHER BACKGROUND CHECKS

HR also conducts other background checks, including criminal records, driving records, and education and professional credentials. For applicants who have adverse background records, HR in collaboration with the hiring supervisor will determine whether the applicant is eligible for employment with Meridian Health Plan, based on the specific role and job function, and the nature of the adverse event or record.

FAIR CREDIT REPORTING ACT (FCRA)

The FCRA requires Meridian Health Plan to provide specific notice, authorization and adverse action procedures for all background checks. The FCRA is designed primarily to protect the privacy of consumer report information and to guarantee that the information supplied by consumer reporting agencies is as accurate as possible. It ensures that individuals are aware that consumer reports may be used for employment purposes, the individuals agree to such use, and individuals are notified promptly if information obtained may result in a negative employment decision.

NOTIFICATION

All applicants, Board members and officers must complete a background authorization form that authorizes HR to conduct background checks. If a decision is made not to hire an applicant due to the applicant being listed on the LEIE or SAM, or due to an adverse background record, HR will provide the applicant with a pre-adverse action disclosure that includes a copy of the adverse background record and a copy of "A Summary of Your Rights Under the Fair Credit Reporting Act." Once the decision is made not to hire the applicant, HR will provide the applicant notice that the action has been taken in an adverse action notice.

PROVIDER & FDR VERIFICATION

Medical Providers: Provider Network checks medical providers against the following data sources at the time of credentialing, monthly, and claim payment to ensure that Meridian Health Plan does not contract

with or reimburse providers who are ineligible to perform work or receive payment for work related directly or indirectly to Federal health care programs:

1. Office of Inspector General (OIG) List of Excluded Individuals and Entities (LEIE)
2. General Services Administration (GSA) System for Award Management (SAM)
3. Medicare Exclusion Database (MED)
4. Medicare Opt-Out

Please refer to Provider Network's credentialing and re-credentialing policy for detail.

Any Medicare claims received from providers, including non-contracted providers, will be checked weekly against the 4 data sources. Provider Network will also verify the providers' Medicare eligibility and enrollment status, and Medicare assignment status. Provider Network will rely on sources such as the National Plan and Provider Enumeration System (NPPES) and www.Medicare.gov to obtain the NPI, taxonomy and PTAN numbers. If a provider is found not be eligible for Medicare payment, the claim will not be paid.

Pharmacy Providers: Pharmacy Services, through its PBM, also screens pharmacies and pharmacists against the exclusion list.

Agents/Brokers: As part of the appointment process, the Sales Department screens agents and brokers against the OIG and GSA list before the agents are allowed to market and sell on behalf of Meridian Health Plan. This screening is also conducted monthly for all contracted agents and brokers.

Attestation: On an annual basis, the Compliance Department will require FDRs performing a core Medicare function to attest and certify their compliance with this requirement. The attestation and certification are subject to validation by the Compliance Department.

SELF-DISCLOSURE

All covered persons are required to immediately disclose to HR any exclusion or other events that make them ineligible to perform work related directly or indirectly to a government health care program. FDRs are to disclose such information to their Meridian Health Plan contract administrator. Failure to disclose may result in appropriate corrective actions, up to and including termination of employment or contract.

REFERENCES

- 42 CFR §422. 204(b)(4), 752(a)(8)
- Chapter 9: Prescription Drug Benefit Manual-Compliance Program Guidelines (§50.6.8)
- OIG
- GSA
- Medicare Opt-Out
- NPPES
- CMS Memo: Excluded Providers (June 29, 2011)
- CMS Medicare Exclusion Database (MED) User Manual (Version 1.0)(May 20, 2011)

POLICY NUMBER C-6B: FDR COMPLIANCE OVERSIGHT

POLICY

Meridian Health Plan is ultimately responsible for actions delegated to first tier, downstream and related (FDR) entities. To that end, Meridian Health Plan maintains adequate and effective oversight over the FDRs to ensure that they comply with applicable regulatory requirements. In addition, this policy outlines certain expectations Meridian Health Plan requires of its FDRs.

PROCEDURE

DEFINITION

Contract Administrator: The business owner responsible for the implementation, operations, oversight and monitoring, and day-to-day relationship with the FDR.

FDR ASSESSMENT & CORE SERVICES

In determining whether an entity is an FDR (and thus the function is delegated) for the purpose of exercising compliance and operational oversight over the entity, the Contract Administrator, in conjunction with the Compliance Department, shall consider the following attributes:

- Whether the entity performs a core service
- Whether the function is a service the plan is required to do or provide under its contract with Medicare (for Parts A, B, C and D services), applicable federal regulations or guidance
- Whether the entity performs an intelligent function, such as analysis and interpretation
- Whether the entity has decision-making authority
- The level of plan intervention and overturn of the entity's decision
- Whether the function directly impacts enrollees
- Whether the entity has direct interaction with enrollees
- Whether the entity has access to beneficiary information or personal health information
- Whether 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 violate Medicare program requirements

Recognizing that it is not feasible to quantify a numerical number of attributes that will trigger FDR status due to the variability in degree and depth of each contractor's responsibility, we will assess an entity against all of these attributes and make a determination based on the most logical and reasonable method.

We do not consider an entity that provides clinical or administrative services pursuant to a supplemental benefit to be an FDR. Supplemental benefit is neither statutorily-mandated nor is it a core service that relates to Medicare Parts A, B, C and D services. The purpose of having an FDR oversight program is to exercise control over entities that administer clinical and administrative services relating to Medicare services. This is done to ensure that members receive timely access to care and the plan is administering its Medicare contract as intended. As such, entities that provide administrative or clinical services pursuant to

a supplemental benefit do not carry the same level of risk and thus do not require the same level of oversight.

The only exception to this rule is for supplemental dental services. While a supplemental service is not related to Parts C or D, it does have a direct impact on a member's timely access to care. Dental claims are also more common, occur in greater frequency and are of a higher-risk than other supplemental benefits, such as vision, transportation, gym and wellness. Untimely dental services may have an adverse medical impact on a member's health that may extend beyond dental, and when compared to other categories of supplemental services that are more for convenience.

Once identified as an FDR, Meridian Health Plan shall exercise oversight over the FDR who performs a delegated, core service on behalf of Meridian Health Plan. A core service is an administrative or health care function related to Medicare Parts A, B, C and D services, and includes such activities as:

- Sales and marketing
- Health care services
- Utilization management
    - Quality improvement
- Enrollment, disenrollment, membership functions
    - Outbound enrollment verification
    - Applications processing
- Claims administration, processing and coverage adjudication
- Generation of claims data
- Pharmacy benefit management
    - Processing of pharmacy claims at the point of sale
    - Administration and tracking of enrollees' drug benefits, including TrOOP balance processing
    - Negotiation with prescription drug manufacturers and others for rebates, discounts or other price concessions on prescription drugs
- Appeals and grievances
- Hotline operations
- Customer service
- Bid preparation
- Provider network management
    - Licensing and credentialing
- Coordination with other benefit programs such as Medicaid, state pharmaceutical assistance or other insurance programs

PRE-DELEGATION ASSESSMENT

Prior to delegating a core service to an FDR, the Compliance Department and the Contract Administrator shall perform, when appropriate, an FDR pre-delegation assessment and review. The review will cover topics such as the FDR's experience in the delegated area, its operational performance, policies and procedures, compliance program infrastructure and adherence, compliance monitoring and auditing, HIPAA Privacy and Security, record retention, reportable metrics, and proof of concept demonstration.

In determining whether to conduct the review, the Compliance Department and the Contract Administrator shall assess the FDR's specific functions, the risks associated with the FDR and functions, and the size and magnitude of the contract.

COMPLIANCE PROGRAM DISSEMINATION

Within **90 days** of contracting, and on an annual basis, the Contract Administrator, working in conjunction with the Compliance Department, shall distribute Meridian Health Plan's Compliance Program and Code of Business Conduct and Ethics to all applicable FDRs. The FDRs may be required to sign an acknowledgment of receipt of the Compliance Program.

FDR COMPLIANCE PROGRAM

Meridian Health Plan also requires certain high-risk FDRs to maintain their own effective compliance program consisting of the 7 core elements. The Compliance Department will (based on our risk assessment) review the FDR's compliance program at the time of contracting, and annually thereafter. Meridian Health Plan may require the FDRs to provide signed attestation/certification of their compliance with this requirement, subject to validation for compliance.

FEDERAL & STATE LAWS

Applicable FDRs must comply with applicable laws and regulations that pertain to government programs, such as HIPAA, Federal False Claims Act, and the Social Security Act. Please see *Policy Number C-1: Compliance with Federal & State Laws* for a detailed list of such laws.

TRAINING

Applicable FDRs must administer effective training and education to all applicable employees who are responsible for the administration or delivery of a government programs at the time of hire and annually thereafter. Training and education must cover general compliance training, specialized compliance training, and FWA training. Please see *Policy Number C-3: Compliance Training* for a detailed description of the training requirements.

COMPLIANCE INVESTIGATION & REPORTING

Applicable FDRs are expected to disclose to Meridian Health Plan potential issues of noncompliance and FWA in a timely manner. FDRs are also expected to cooperate with Meridian Health Plan in the investigation and resolution of such issues. Upon discovery of an incident or report of a potential noncompliant or FWA issue, the FDR is expected to initiate a thorough investigation of the incident. All applicable deficiencies and instances of noncompliance must be tracked and monitored by formal corrective action plans (CAP) to ensure that they are remedied and are not likely to reoccur. Please see *Policy Number C-4: Effective Lines of Compliance Communication, Reporting & Non-Retaliation* for a detailed description of the reporting process.

In addition, the FDR must maintain effective lines of communication within its organization to ensure that its employees raise compliance issues, and provide a means for anonymous and confidential good faith reporting of potential compliance issues as they are identified.

Lastly, the FDR must support a non-intimidation and non-retaliation environment that allows individuals to make good faith reports without repercussion or fear of retaliation. Those who retaliate against an individual who makes a good faith effort to report a compliance or FWA issue will be subject to the FDR's disciplinary actions.

DISCIPLINARY STANDARDS

Applicable FDRs must maintain disciplinary standards to ensure that their employees who commit a compliance or FWA violation are subject to disciplinary and corrective actions, up to and including termination.

MONITORING & AUDITING

Meridian Health Plan requires applicable FDRs to conduct self-monitoring and self-auditing of their operational performance, remedy all identified areas of deficiency, and disclose them to Meridian Health Plan. In addition, the Contract Administrator is obligated to oversee and routinely monitor the FDR's work performance and compliance relative to its delegated functions.

The Compliance Department also routinely monitors and assesses the FDR's operational performance as it relates to compliance measures. Please see *Policy Number C-6: Compliance Monitoring & Auditing* for a detailed discussion of the monitoring and oversight activities.

GENERAL OVERSIGHT

Performance Metrics: Applicable FDRs are required to provide and report to the Contract Administrator (and the Compliance Department as appropriate) operational performance metrics that reflect the FDR's compliance with regulatory and business standards.

Routine Meetings: Applicable FDRs are expected to maintain regular operational or management meetings with the Contract Administrator (and the Compliance Department when appropriate) to ensure issue resolution, process enhancements, and coordination of communication.

Post-Implementation: On a risk basis, the Compliance Department may conduct a post-implementation review approximately **60 days** after the initial go-live date. This is done to ensure that the FDR is performing in accordance with State, Federal and Meridian Health Plan standards and business expectation, and that issues are identified and remediated early in the contract relationship.

REFERENCES

- Chapter 9: Prescription Drug Benefit Manual-Compliance Program Guidelines (§40)

POLICY NUMBER C-7: COMPLIANCE INVESTIGATION & CORRECTIVE ACTION PLAN

POLICY

Upon discovery of an incident or report of a potential noncompliance or fraud, waste and abuse (FWA) issue, the Compliance Department will initiate a thorough investigation of the incident. All applicable deficiencies and instances of noncompliance are tracked and monitored by formal corrective action plans (CAP) to ensure that they are remedied and are not likely to reoccur.

DEFINITIONS

Abuse: Any action that may, directly or indirectly, result in unnecessary costs to the Medicare and Medicaid 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.

Fraud: 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.

Waste: The overutilization of services, misuse of resources, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare or Medicaid Program.

Examples of cases that pertain to FWA include:

- Services not rendered
- Lack of medical necessity
- Services misrepresented
- Fraudulent billing schemes
- Identity theft
- Kickbacks and self-referrals

PROCEDURE

SOURCES OF INCIDENT REPORTING

The Compliance Department investigates all incidents and reports of noncompliance or FWA issues that may come from formal and informal communication channels. In addition, incidents and reports of noncompliance or FWA issues may also come from various sources, including:

- Regulatory agencies such as CMS, OIG, NBI MEDIC, DOJ, law enforcement
- National fraud alerts
- Complaint Tracking Module (CTM)
- Prospective claim review
- Retrospective data mining
- Employee reporting

- Member reporting
- First tier, downstream and related entity (FDR) reporting
- Compliance monitoring/audit findings
- Opt-out & exclusion list screening
- Employer client reporting
- EthicsPoint
- HR exit interviews or questionnaire

To that end, Meridian Health Plan maintains these open lines of communication channels and routinely monitors them for reports of potential incidents.

INVESTIGATIVE PROCESS

Investigation of all incidents and reports are initiated within **2 weeks** of the date the incident was identified or reported. If a department or individual (other than the Compliance Department) receives a reported incident, that department or individual is responsible for gathering the relevant facts and referring the matter over to the Compliance Department when applicable.

Upon initiating an investigation, the issue or incident will be assigned to a Compliance Department investigator. The investigator will complete either a CAP or Compliance Investigation Form to document its course of action. During the investigation process, the Compliance Department will utilize any of the following methods:

- Interviews
- Review of process and system
- Review of policies and procedures
- Risk analysis
- Root cause analysis
- Beneficiary, financial, or operational impact analysis
- Validation of sample cases

Cases are resolved as expeditiously as possible depending on the complexity and issue at hand. Complexity is based on factors such as the risks involved, amount of data and facts to be researched and confirmed in order to form a conclusion, clarity of issue and root cause, actions needed to resolve the issue, and the available resources. Every single case varies by fact, circumstance, complexity, and resource availability. Thus, it is sometimes not possible to close out a case within a strict and defined timeframe because doing so will compromise the integrity, quality and thoroughness of an investigation. To that end, we adopt a "reasonable" approach to timely resolution of cases. The following are suggested guidelines for closing out a case.

Complexity Level 1 [Simple]: Within **2 months**
Complexity Level 2 [Complex]: Within **6 months**
Complexity Level 3 [Highly Complex]: Within **6-12 months**
Complexity Level 4 [Exceptionally Complex]: Over **12 months**

The case will be designated a complexity level. We reserve the right to change the complexity level throughout the investigation as the situation warrants with proper documentation justifying the change.

FWA DATA MINING & ANALYSIS

Meridian conducts data analysis through the use of data mining tools to prevent, detect, and correct noncompliance and FWA. We utilize payment integrity tools to detect FWA schemes, algorithms and aberrant patterns and behaviors at the member and provider level, such as:

- Fraud alerts
- Retrospective DUR claim audits
- Concurrent DUR claim audits
- Member drug abuse audits
- Pharmacy audits

Meridian reviews member, physician, and pharmacy prescriptions and claims for potential FWA issues, such as high quantities of controlled substances, high cost utilization, multiple prescriber utilization, and multiple pharmacy dispensing. See the *FWA Data Mining & Resolution Process* for detail.

PROVIDER FRAUD ALERT INVESTIGATION

The following procedures are established to review, investigate and analyze provider fraud alerts.

1. On a monthly basis, the Compliance Department checks the following websites for national fraud issues:
    a. U.S. Department of Justice
    b. Medicare Fraud Strike Force
2. If fraud alerts are issued directly to plans (i.e., through HPMS or CMS), initiate investigation within **2 weeks** of the issuance.
3. When necessary, verify the suspect provider's information, including NPI, through:
    a. NPI Registry
    b. Medicare Physician Lookup
    c. OIG Exclusions List
    d. Federation of State Medical Boards
    e. Secretary of State website
    f. State licensing/medical board website
4. Verify the provider's contract status with Provider Network
    a. If no match, retain screen print or document "no match" finding and follow Step 8.
    b. If positive match, document in Step 7
5. Run claim analysis against claim systems
6. If no match, retain screen print of "no match" finding and follow Step 8
7. If positive match:
    a. Create impact analysis to claim dollar, member, and provider
    b. Report all positive match findings to FWA Committee with action plan to recover/recoup, suspend/terminate provider, and other appropriate actions
    c. The FWA Committee then follows its procedure
8. Provide monthly summary report to the Compliance Officer

SIU & FRAUD COMMITTEE

Purpose: Meridian maintains a Special Investigation Unit (SIU) and FWA Committee that oversee the implementation and enforcement of detected FWA issues stemming from sources such as data mining and claim monitoring and audits.

Reporting & Accountability: The Associate General Counsel/Vice President of Legal oversees the Fraud Committee and reports to the Compliance Committee on its behalf.

Membership: The Fraud Committee maintains memberships from a variety of backgrounds, including Pharmacy Services, Health Services, Provider Network, and Claims.

Roles & Responsibilities: The Fraud Committee maintains the following, but not limited, roles and responsibilities:

1. Meet at least quarterly to review and discuss FWA issues.

2. Triage, review and analyze FWA issues stemming from sources such as data mining, claim monitoring and audits, and Federal and State fraud alerts.

3. Make recommendations to recoup, suspend or terminate suspect providers, members, or any individual(s) found to have violated a FWA issue.

4. Make recommendations to refer matters to the NBI MEDIC, CMS, OIG, DOJ, law enforcement, State Medicaid Fraud Control Units (MCFU), State licensing boards, the National Practitioner Data Bank (NPDB) when applicable, and assist law enforcement by providing information needed to develop successful prosecutions.

5. Reduce or eliminate benefit costs due to FWA.

6. Ensure proper value of health services, including correct pricing, quantity, and quality.

7. Utilize real-time systems that ensure accurate eligibility, benefits, services, refills, and pricing and that identify potential adverse drug interactions and quality of care issues.

8. Monitor fraudulent or abusive paid claims and take appropriate actions when necessary.

9. Prevent illegal activities.

10. Identify members with drug addiction problems and other overutilization issues and take appropriate actions when necessary.

11. Provide fraud awareness training to applicable individuals.

12. Support the Compliance Department in its duty to carry out FWA activities.

13. Report to the Compliance Committee through the Compliance Officer on results and plan of action on suspect FWA cases.

14. Make recommendation to initiate recovery and recoupment of claim dollars.

15. Make recommendation to suspend, sanction or terminate a provider.

REFERRAL, DISCLOSURE & COORDINATION WITH EXTERNAL AGENCIES

Meridian Health Plan will refer matters over to Federal and State regulatory agencies and law enforcement, including the National Benefit Integrity Medicare Drug Integrity Contractor (NBI MEDIC), under certain circumstances, including:

- Incidents it does not investigate due to resource constraints
- Potential criminal, civil, or administrative law violations
- Allegations involving multiple health plans, multiple states, or widespread schemes
- Allegations involving known patterns of fraud
- Pattern of fraud or abuse threatening the life or well-being of beneficiaries
- Scheme with large financial risk to the Medicare program or beneficiaries

The referral will include certain information, if it is available, such as:

- Organization name and contact information
- Summary of the Issue
    - Information on who, what, when, where, how, and why
    - Any potential legal violations
- Specific Statutes and Allegations
    - List of civil, criminal, and administrative code or rule violations, state and federal
    - Detailed description of the allegations or pattern of FWA
- Incidents and Issues
    - List of incidents and issues related to the allegations
- Background information
    - Contact information for the complainant, the perpetrator or subject of the investigation, and beneficiaries, pharmacies, providers, or other entities involved.
    - Names and contact information of informants, relators, witnesses, websites, geographic locations, corporate relationships, networks.
- Perspectives of Interested Parties
    - Perspective of Plan, CMS, beneficiary
- Data
    - Existing and potential data sources
    - Graphs and trending
    - Maps
    - Financial impact estimates
- Recommendations in Pursuing the Case
    - Next steps, special considerations, cautions

Cases to the NBI MEDIC are referred within **30 days** (when possible) of the date the incident was identified or reported.

NBI MEDIC: Health Integrity, LLC

28464 Marlboro Avenue
Easton, Maryland 21601-2732
1-866-886-2658

Meridian Health Plan will provide additional information pursuant to the MEDIC's request within **30 days**, or within a timeframe required by the MEDIC. In addition, the Compliance Department may disclose incidents of significant or serious compliance and FWA violations to CMS, the NBI MEDIC, the OIG, and the Department of Justice when appropriate and warranted.

In addition, the Compliance Department will refer, report and coordinate with State Medicaid Fraud Control Units (MFCU) on issues impacting Medicaid. Meridian Health Plan shall refer member and provider fraud cases, including those referred by the member or provider, to the following agencies:

General: http://oig.hhs.gov/fraud/medicaid-fraud-control-units-mfcu/files/contact-directors.pdf
http://oig.hhs.gov/fraud/medicaid-fraud-control-units-mfcu/index.asp
https://oig.hhs.gov/fraud/report-fraud/index.asp
http://namfcu.net/medicaid-fraud-control-unit1.php
https://www.medicare.gov/forms-help-and-resources/report-fraud-and-abuse/fraud-and-abuse.html

If Meridian Health Plan is aware that there are credible allegations of fraud for which an investigation is pending against a provider, Meridian Health Plan may terminate the contract or suspend payments to the provider unless we determine there is good cause not to terminate or suspend payments.

FRAUD ALERTS

Upon receipt of a fraud alert from CMS, OIG, the MEDIC, or any State and Federal government agency, the Compliance Department shall investigate the matter, analyze the claim system for potential impact, and deny, reverse and recoup impacted claims based on internal analysis. Compliance will work with the Pharmacy Services and the PBM to identify potential fraudulent claims and correct PDE data submissions.

Provider Network, working in conjunction with the Compliance Department, shall review the contractual agreements with the identified providers and may initiate termination if law enforcement has issued indictments against those providers.

SUSPECT PROVIDER LIST

The Compliance Department maintains for a period of **10 years** a suspect list of in-network and out-of-network providers who have been the subject of complaints, investigations, violations, and prosecutions. This includes potential suspicious activities identified as part of our internal FWA program, enrollee complaints, CMS fraud alerts, internal investigations, NBI MEDIC investigations, OIG and/or DOJ investigations, US Attorney prosecution, and any other civil, criminal, or administrative actions taken stemming from a violation of Federal and State health care program requirements. The screening process is as follows:

1. On a monthly basis, the Compliance Department provides Provider Network and Claims Department (medical and pharmacy) with an updated list based on new providers identified, in addition to existing.

2. The Claims Departments (medical and pharmacy) review the list for claim impact.
3. At **initial credentialing**, Provider Network Contracting screens applicant providers against the suspect list and may deny the application based on the conduct, as determined by Provider Network.
4. During **re-credentialing**, Provider Network Credentialing also screens contracted providers on the suspect list against providers who are being considered for re-credentialing to determine if any concerns should be considered when presenting the credentialing file to the Credentialing Committee for review. The Credentialing Department also screens currently-credentialed providers against the suspect list to determine if any corrective action is warranted. Corrective actions may include provider remedial education, suspension, and termination. The screening of currently credentialed providers is not limited to the 3 year credentialing cycle and may be reviewed more frequently, as needed.
5. To measure the effectiveness of the suspect list, the Claims Departments and Provider Network provide the Compliance Department with routine updates on the follow-up actions should the suspect list result in any positive hit, regardless of the final outcome.
6. While the suspect list is retained for 10 years, we employ a **3 year** look-back period to canvass new suspect providers. This is done to balance resource constraints but still maintain a robust fraud program.

COORDINATION WITH HUMAN RESOURCES

For issues that have an impact on personnel matters, Human Resources will be engaged appropriately to handle compliance or FWA issues that impact such personnel matters.

DOCUMENTATION & PROVIDER FILE MAINTENANCE

The Compliance Department will retain documentation of investigations, including the original documentation of reports of noncompliance and FWA violations. The Compliance Department will retain investigative documents on providers who were the focus of an internal investigation. In addition, we will also maintain files on applicable providers who have been the subject of complaints, investigations, violations, and prosecutions stemming from enrollee complaints, fraud alerts, NBI MEDIC investigations, OIG and/or DOJ investigations, US Attorney prosecution, and any other civil, criminal, or administrative action for violations of Federal health care program requirements.

Meridian Health Plan shall permit Federal and State agencies to inspect, evaluate, or audit books, records, documents, files, accounts, and facilities maintained by or on behalf of Meridian Health Plan or by or on behalf of any FDR, as required to investigate an incident of fraud and abuse.

Meridian Health Plan shall cooperate, and requires its FDR to cooperate, with Federal and State investigators during any investigation of fraud or abuse.

In the event that Meridian Health Plan reports suspected fraud or abuse by an FDR, or learns of a Federal or State investigation of an FDR, Meridian Health Plan should not notify or otherwise advise its FDR of the investigation. Doing so may compromise the investigation.

Meridian Health Plan shall provide copies of reports or other documentation, including those requested from the FDR regarding the suspected fraud or abuse at no cost to the Federal and State agencies during an investigation.

INVESTIGATIVE FINDINGS

At the conclusion of the investigation into the incident, the Compliance investigator will document the findings. If it is determined that the incident does not warrant a formal corrective action plans (CAP), the Compliance investigator will document the rationale supporting this decision. Otherwise, a formal corrective action plans (CAP) will be implemented and tracked until remediation.

FWA CLOSURE

If a case qualifies as fraud, waste or abuse, it will be noted as such and follow the documentation process as outlined in the **CAP CLOSURE** section of this policy. The following factors will determine if the case will follow the process:

- It meets the definition of FWA, as defined in this policy
- The identified provider is contracted (regardless of claim history)
- The identified provider has claim history (regardless of contract status)
- All cases that were forwarded to law enforcement and external agencies

CORRECTIVE ACTION PLAN

CAPs are generated due to deficiencies and incidents of noncompliance, and may arise from various sources, including:

- Routine monitoring
- Internal audits
- External audits
- Investigations
- Self-disclosure
- Reporting
- Regulatory agency initiatives

Upon discovery of a compliance or FWA issue, the Compliance Department will initiate an investigation into the matter. We will then determine whether the issue warrants opening a formal CAP. Considerations to opening a CAP include, but are not limited to:

- Nature of violation
- History of violation or recurrence
- Risk to beneficiary access to care and protection
- Risk of government sanctions, fines, and corrective actions
- Likelihood of recurrence
- Root cause (i.e., manual/human error, process/systemic problem)

CAP CREATION

If a formal CAP is required, the Compliance Department will enter all relevant information into the CAP Database. The CAP will then follow the following process:

1. Compliance will notify business owners of the opening of a CAP by sending an email with a link to the SharePoint site and a partially-complete CAP form. Once the CAP form is initiated by Compliance, business owners must investigate the errors or deficiencies and complete the appropriate sections of the CAP form within the following timeframes:

    a. **7 days** from receiving the CAP form from Compliance. This standard timeframe applies to most issues.
    b. **30 days** from receiving the CAP form from Compliance. This exceptional timeframe applies only to a small number of highly complex issues, and must only be used on a limited basis, such as:
        i. When the resolution is complex or unknown and will require time to investigate.
        ii. When the resolution is co-dependent on substantial resource allocation, or system/software enhancement or purchase and will require time to investigate.
        iii. When there are other good business rationales.

    The business owner will be largely responsible for completing the Interim Activities and Corrective Action Plan sections of the form. By the form due date, these sections, and any other sections requiring business owner input, should be completed. This allows Compliance to ensure that the root cause of the non-compliance will be addressed and that the corrective action is appropriate.

2. Compliance may open multiple Corrective Actions if numerous deficiencies are found within the same business area. When possible, Compliance will combine issues into one CAP form. However, for clarity, tracking and documentation purposes multiple CAPs may be needed.

3. The CAP is sent electronically to the business owner of the affected area, and may also be distributed to the associated supervisor, manager and/or executive. This electronic communication will contain a link to the SharePoint site and CAP form.

4. Once the CAP form is completed, it is then reviewed by the compliance owner for appropriateness and completeness of the proposed corrective actions and timelines. If any adjustments to the CAP are required, the compliance owner will discuss the issue(s) with the business owner(s) and reach agreement on appropriate corrective action. If the CAP form is not completed timely, follow-up requests will be made to management of the affected area. All follow-up attempts for information will be documented by the compliance owner within the comments section of the CAP form. If the CAP form is not complete, the CAP will be reported as at risk as described in the reporting section below.

CAP TIMELINES

The standard timeline for issue resolution of a CAP will default to **30 days**. However, there may be operational and other circumstances which will require longer timelines. It is up to the business owners to designate an appropriate timeline (that may exceed 30 days to resolve) at the time the CAP is created. Timelines that exceed **90 days** will be subject to greater scrutiny and will be reported to Compliance Committee as a potential risk issue. In determining the appropriate timeline, the business owners must make a good faith effort to calculate a reasonable, achievable and realistic timeline to resolve the CAP based on objective criteria. Compliance will work with the business owners on a mutually-acceptable, achievable

and realistic timeframe while being mindful of the potential risks and urgencies created by the non-compliance.

CAP TIMELINE REVISION

The original timeline may be revised after the CAP has been opened for good cause. Examples of good cause may include:

- The resolution becomes more apparent in complexity or impact during the CAP process, and this was not foreseeable when the CAP was first opened.
- Resource, staff or system constraints that were not foreseeable when the CAP was first opened.
- Other good business rationale.

Requests to revise the CAP timeline must be made before the original CAP timeline expires. The CAP timeline will not be revised for the following reasons:

- Lack of good faith due diligence in resolving the CAP during the original timeline.
- Inadequate administration of resource or timing to resolve the CAP.

Revising the original CAP timeline has the effect of keeping the CAP at *On Track* status.

CAP EXTENSION

Business owners may request an extension to a CAP. An extension differs from a revised timeline in that an extension provides a short-term period to resolve minor, low risk issues that may prevent the CAP from being resolved in its entirety, while a revised timeline is a long-term period that is needed to resolve the fundamental essence of the CAP.

Business owners may request an extension for good cause. Examples of good cause may include:

- Minor resource, staffing or system issues that prevent the CAP from being closed in its entirety.
- Other good business rationale.

Requests for extension must be made before the CAP timeline expires. Extensions will not be made for the following reasons:

- Lack of due diligence in resolving the CAP during the original timeline.

An extension has the effect of keeping the CAP at *On Track-Extension* status, but maintaining the original timeline. All requests for CAP Timeline Revisions and CAP Extensions must be documented in the actual CAP status update.

CAP TRACKING

Compliance will track the CAP progression on a continuous basis. CAPs are tracked based on Stage and Status:

Stage: This tracks where the CAP is in its lifecycle:

- **Stage 1 [In Progress]:** The issue is currently being worked on to be resolved.

- **Stage 2 [Issue Resolved/Validation]:** The issue is resolved from an operational perspective. While the issue may be resolved, the CAP may still be open pending validation. The issue is being validated to confirm that it has been resolved. Depending on risk, some issues require validation before it can be closed, through monitoring or auditing.
- **Stage 3 [Closed]:** The CAP is fully resolved and is closed.

Status: This tracks where the CAP is in its deadline:

- **On Track:** The CAP is on-track to be resolved timely based on its original deadline.
- **On Track-Extension [number of extensions taken]:** The CAP is on-track to be resolved timely based on its extended deadline. The status will show the number of extensions taken on the CAP.
- **Late:** The CAP is in late status.

At risk status indicates that the CAP will likely not meet the resolution deadline due to lack of form completion, business owner attention or other circumstances. Business owners will be required to update the CAP as issues are resolved. The SharePoint system will generate due date reminders 7, 3 and 1 day prior to the resolution due date. These reminders will be sent to the business owner, the applicable Executive Leadership, and the compliance owner. Once the plan has been effectuated and all errors and deficiencies addressed, the CAP form will be marked as completed and closed.

CAP ESCALATION

CAPs that are untimely and in *Late* status will be escalated to the next level of management, including the Executive Leadership overseeing the business area. Untimely and high-risk *Late* CAPs will also be escalated and reported to the Compliance Committee, Executive Leadership and Board of Directors. Failure to resolve a CAP timely and in its entirety may result in disciplinary action up to and including termination or dismissal of the responsible party, or termination of contract.

CAP REPORTING

The Compliance Officer will report to the Compliance Committee relevant open and closed CAPs that were initiated within the last 30 days. Special emphasis will be given to those CAPs that are in *On Track-Extension*, *At Risk* or *Late* status.

CAP CLOSURE

If it is determined that the issue has been remediated, the Compliance Department will close out a CAP. Prior to closing a CAP, we will analyze the CAP against the 7 elements of an effective compliance program. The following analysis (except for Element II) must be initiated within **1 month** (when possible) of the business owner's confirmation that the issue has been remediated:

- **Element 1:** We will assess whether operational and compliance policies and procedures existed before the issue occurred, and whether they have been created or revised to address the issue.
    - The original operational and compliance policy will be uploaded to the CAP database. Compliance requires that all issues have an underlying written policy or process.
    - The revised operational and compliance policy will be uploaded to the CAP database. An acceptable rationale must be provided if no revision was made.

- **Element II:** We will report high-risk CAPs to the Compliance Committee, Executive Leadership and CEO as appropriate.
    - For each committee, documentation is maintained separately in its respective SharePoint documentation folder.
    - All issues are presented to the Compliance Committee.
    - Recognizing that the Board of Directors and the CEO function at a higher level, if the issue is not reported to them (such as due to low risk or low impact), an acceptable rationale must be documented.
    - Directives and follow-up instructions from the CEO or Board of Directors related to the issue are documented in their respective minutes.
- **Element III:** We will require business owners to conduct operational training and education with staff on the new process for high-risk CAPs. An acceptable rationale must be provided if no training was conducted.
- **Element IV:** Evidence of communication may be emails from the Compliance Officer/Department to business owners, and issues log and final audit report dissemination.
- **Element V:** We will assess whether the business owner took disciplinary actions against personnel due to the CAP. An acceptable rationale must be provided if such actions did not occur.
- **Element VI:** We will conduct a risk assessment of the issue to determine what level of validation (monitoring/auditing) is needed before closing out a CAP:
    - *Medium Risk*: The CAP has marginal impact on members or compliance. The CAP can be closed with documentation of routine monitoring.
    - *High Risk*: The CAP has significant member or compliance impact, or is a repeat finding, and requires documentation of routine monitoring and auditing before it can be closed.

  If the issue was not previously identified in our initial risk assessment (and thus not incorporated into the compliance workplan), the CAP will document a new risk assessment to determine if it needs to be incorporated into the compliance workplan as a new addition.
- **Element VII:** The actual CAP articulates the prompt response to compliance issues. The CAP documents the following:
    - Root cause analysis.
    - Corrective actions taken.
    - Timeline of corrective actions.

Documentation and rationale for each element will be documented in the actual CAP database under their respective element data fields. If an element does not apply, or an activity was not performed in support of the element, the rationale will be noted in the element data field. With the exception of Element II, a CAP cannot be closed until all elements have been assessed. Due to timing, issues may be reported to the Compliance Committee, Board of Directors, and CEO at a later date.

If an issue has a negative member impact, the member shall be made whole when appropriate. If the issue has a negative impact to CMS or a State or Federal regulatory agency, those entities shall be made whole when appropriate.

Violations that stem from an employee or FDR's failure shall be handled in accordance with the disciplinary guidelines and enforcement standards.

ONGOING MONITORING & AUDITING

Depending on the nature, extent and risk of the issue, the Compliance Department may conduct, or require business owners to conduct, ongoing monitoring reviews to measure the effectiveness of the resolution and to ensure that the issue is not likely to reoccur.

We may audit the business owners and verify that the solutions put in place are satisfactory to remediate the deficiency. We may review, audit and verify activities such as process improvements, business efficiency analysis, root cause analysis, internal controls, and any other parameters that may impact the business area's compliance and business operations.

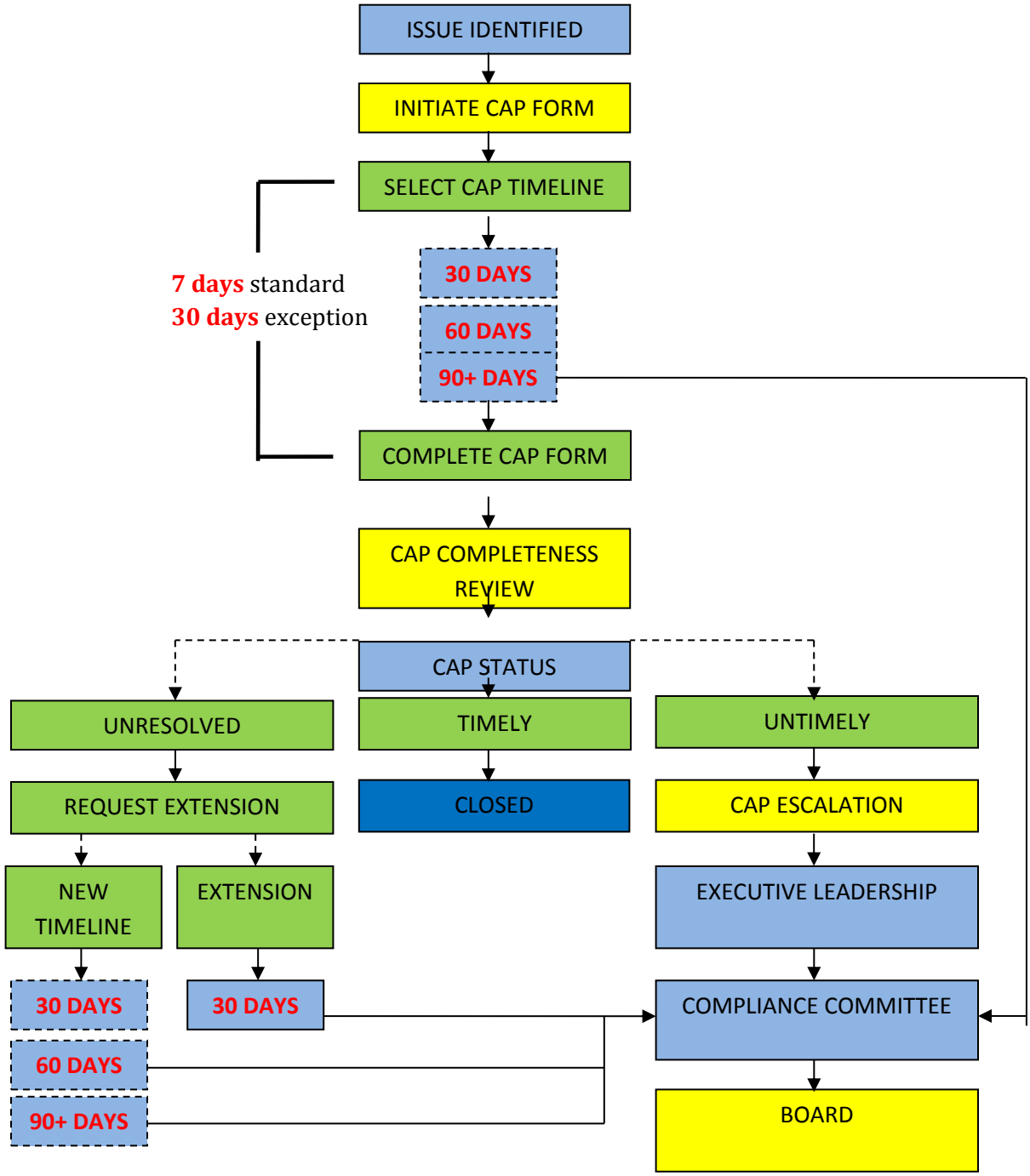
REFERENCES

- Chapter 9: Prescription Drug Benefit Manual-Compliance Program Guidelines (§50.1.6, 50.7)
- OIG Self-Disclosure Policy

Shared responsibility (Business Owner & Compliance)

Business Owner

Compliance



STANDARDS OF CONDUCT

Meridian Health Plan has a history of succeeding through honest business competition. We do not seek competitive advantages through illegal or unethical business practices. Meridian employees, representatives and business partners must endeavor to deal fairly with state and federal agencies, Meridian's customers, service providers, suppliers, and competitors. We do this by adhering to the expectations set forth in this document.

We expect our employees, representatives and business partners to perform their duties in compliance with this Standards of Conduct. It is your responsibility to immediately report any potential compliance violation. While there is no single standard that governs all situations, the use of available resources, good judgment and common sense combined with personal integrity and honesty is the best guide to assure that business activities are conducted with the highest ethical standards.

APPLICABILITY

This document applies to all Meridian employees, Board of Directors, committee members, temporary staff, students, interns, externs, clinical residents, and first tier, downstream or related entities ("FDR"), collectively referred to as "covered persons". This document addresses standards in the areas of personnel conduct, compliance and fraud waste and abuse (FWA).

BOARD OF DIRECTORS APPROVAL

To show our commitment to ethical behavior, this document is reviewed and approved by the Board of Directors on an annual basis.

LEADERSHIP RESPONSIBILITY

Leadership entails special responsibilities. Meridian leaders are responsible for making strategic business decisions that align with our ethical standards. In addition to setting the tone at the top, leaders must be knowledgeable about the content and operation of the Compliance Program. The leadership team plays an important role in building integrity, respect, credibility and long-term sustainability for the Company. Because leadership sets an example for all employees, they must:

- Foster an environment of transparency
- Maintain a positive, ethical work environment
- Make certain that employees understand what is expected of them both professionally and ethically
- Maintain an open door policy on a routine basis for employees to ask questions and raise concerns
- Address issues raised by employees by listening and taking action, when appropriate
- Be fair and objective
- Be a positive role model

TRAINING AND ACKNOWLEDGMENT

To ensure full understanding of the Standards of Conduct, all covered persons must read this document within **90 days** of hire/contracting and/or placement, and annually thereafter. If you are an FDR, you must distribute a copy of this document to your employees and contractors upon hire/contract/placement, and annually. All covered persons must also complete an Acknowledgment Form to confirm that you have read and understood our expectations as set forth in this document.

REPORTING AND NON-RETALIATION

You are expected and required to report any suspected violation or ethical problem to any of the appropriate channels listed in this document. You have a right to report anonymously and we will protect your anonymity to the greatest extent possible within the confines of the law, regulation, or court order.

Meridian will not retaliate against any person on the grounds that he or she reports a violation or makes a complaint in good faith, or if the person cooperates with an investigation or otherwise provides information. If a Meridian employee violates this non-retaliation policy, disciplinary action may be taken as necessary. Managers and other employees in leadership roles must foster a culture of openness and disclosure and be in-tuned to potential issues, actual or perceived.

Furthermore, if you are filing a qui tam action under the Federal False Claims Act, you are protected by law from being discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in your employment as a result of filing a qui tam action.

INVESTIGATION & RESOLUTION

If your report pertains to a compliance or FWA issue, the Compliance Department will start the investigation within **2 weeks** of the report. During the investigative process, we will conduct interviews, do a risk analysis, analyze the root cause, review processes and systems, and assess the impact to the beneficiary/member, government, and the organization.

At the conclusion of the investigation, we will document the findings. If the incident warrants, we will issue a formal corrective action plan (CAP) to track and remedy the issue. We may refer serious matters over to federal and state regulatory agencies, including law enforcement. We will make every effort to inform you of the outcome of the investigation, subject to legal or confidentiality constraints.

CONFLICTS OF INTEREST

A "Conflict of Interest" is any circumstance that would cast doubt on your ability to act with total objectivity with regard to Meridian's interests. You may have a conflict of interest if your private activities or interests could interfere or appear to interfere with the actions or decisions that you conduct on behalf of Meridian. You must avoid actual or apparent conflicts of interest as they may damage Meridian's reputation and jeopardize your ability to perform your job objectively.

You must disclose potential conflicts of interest within **30 days** of hire, contracting, placement or appointment, within **30 days** of discovering the conflict, and annually thereafter to Human Resources or your Meridian contract administrator.

If it is determined that a conflict of interest exists, you may be asked to correct the situation that gave rise to the conflict. This includes terminating or recusing yourself from the position, disbursing or selling any financial interest, or repositioning your position or job function.

For our directors and executive officers, a waiver to this policy can only be granted by the applicable Meridian Board of Directors based on good cause. For all others, a waiver can be made by the General Counsel or Chief Administrative Officer in conjunction with management.

Board of Directors

As a member of the Board of Directors you may have a conflict of interest if you possess an interest or take an action that makes it difficult to perform your duties in an objective manner, or if you or a family member receives improper personal benefits as a result of your position as a Meridian director.

The Board of Directors should remain vigilant in recognizing situations that may lead to possible conflicts, including any proposed affiliation with a for-profit organization or any proposed transaction involving Meridian where a director has a direct economic or beneficial interest.

All Other Covered Persons

To protect the best interests of Meridian, you must avoid situations where your personal interest could conflict or appear to conflict with your responsibilities, obligations or duties to further Meridian's business interests. This includes situations that could present an opportunity for personal gain apart from the normal compensation provided through employment or placement. Anything that would present a conflict for you would likely also present a conflict if it is related to a family member.

You are prohibited from participating in outside activities or possessing ownership interests that may create conflicts of interest or otherwise interfere with your ability to perform your duties. If you or a member of your family have any of the following kinds of interests, you must notify your supervisor/contract administrator and Human Resources:

- Acting as an employee, officer, director, consultant, or agent with any business, nonprofit organization, or government entity that competes with Meridian, or is one of Meridian's customers, providers, or vendors.
- The acquisition of a significant ownership interest in any business that competes with Meridian, or is one of Meridian's customer, providers, or vendors. A "significant ownership interest" is five percent or more of any business.
- Conducting business on behalf of Meridian with a member of your family or a close friend or with a business organization in which a family member or close friend has a significant ownership interest.

EMPLOYMENT RELATIONS AND WORK ENVIRONMENT

Meridian is committed to providing a professional work environment that maintains equality, dignity and respect. In keeping with this commitment, Meridian strictly prohibits discriminatory practices, including sexual harassment as well as harassment due to race, color, religion, national origin, ancestry, age, gender, height, weight, marital status, physical or mental disability or any other status or condition protected by applicable state or federal law. Meridian expects its FDRs to adhere to the same standards.

Equal employment opportunity

Meridian prides itself on being an Equal Opportunity and Affirmative Action employer. We recruit, hire, train and promote persons in all job classifications based on an individual's qualifications, skills, and performance, without regard to any status or condition protected by applicable state or federal law.

Meridian strives to ensure that all personnel programs such as compensation, benefits, transfers, layoffs, return from layoff, company-sponsored training, education, and social and recreational programs are administered equally and without regard to any status or condition protected by applicable state or federal law. It is our goal to have a workforce that reasonably reflects the diversity of qualified talent that is available in relevant labor markets.

Non-discrimination/harassment

Inappropriate behavior including any sexual or other unlawful harassment, whether verbal or physical, is unacceptable and will not be tolerated, whether it occurs in the workplace or in conjunction with an outside work-sponsored event or activity.

You are required and expected to treat others with respect. Unwelcome or potentially offensive or abusive verbal or physical behavior is not tolerated, including slurs, jokes, name-calling, unwanted physical contact, or any other harassing or intimidating behavior.

Supervisors are required to administer Meridian's policies and procedures in a consistent, non-discriminatory manner, and are expected to monitor their work environment to preemptively address any inappropriate or harassing behavior.

If you believe you have been harassed or discriminated against or if you witness harassment or discrimination against another employee, contact HR as soon as possible. All claims of harassment and discrimination are serious and will be treated as such.

Workplace violence and weapons-free workplace

We are committed to providing a safe and healthful work environment. Therefore, Meridian prohibits any acts or threats of violence by any employee or former employee against any other employee at any time, whether it is work-related or not, on or off premise. We also will not condone any acts or threats of violence against our members or visitors in or around Meridian facilities or elsewhere at any time.

The possession and/or use of weapons by unauthorized persons in or around Meridian property is forbidden. If you believe that you have experienced or witnessed inappropriate behavior, you must report it to your supervisor/contract administrator, security personnel, or HR.

Drug and alcohol free workplace

Meridian's commitment to health and safety compel us to maintain a drug and alcohol free workplace. You are required to perform all your job duties free from the influence of drugs or alcohol. Meridian prohibits the unlawful manufacture, distribution, dispersion, sale, transfer or possession, or use of any illegal or unauthorized controlled substance by employees. The Drug/Substance Abuse policy applies while you are on Meridian property and while you are doing Meridian business anywhere.

Personal relationships

Meridian understands that close personal relationships may develop in the workplace. If you have such a relationship with a person in your reporting line, you must disclose that relationship to Human Resources. Human Resources will make a determination as to whether reporting relationships need to be modified, and how best to address the situation in a fair manner for all parties.

Use of Meridian property and resources

You must use Meridian property and resources, including, but not limited to, e-mail, Internet, software and applications, and telephones only for Meridian business. Personal phone calls must be kept to a minimum and should be placed on personal time, during breaks and lunch periods, except for emergency situations. If you think Meridian property or resources are being misused, contact HR.

Monitoring

Meridian may monitor, intercept, and search and seize any communication or data transiting or stored on its information systems. This includes e-mail, Internet usage, personal computer files, or any personal effects stored at Meridian work stations or otherwise on company property. All phone calls made to and from Meridian phones are recorded. Meridian may perform such monitoring or inspections at any time for any company purpose, including to comply with the terms of company policies and procedures.

BUSINESS AND TRADE PRACTICES

Meridian takes great pride in being awarded government contracts and take the responsibility of administering these contracts very seriously. We must always conduct ourselves in full compliance with any laws, regulations, or rules of ethics that apply to our business. We must demonstrate the highest standards of conduct and integrity. Our FDRs supporting our government contracts are expected to hold themselves to the same standard.

Compliance with these rules is critical to Meridian's success as a business and our commitment to ethical business practices. The following are important guidelines to keep in mind when performing Meridian business:

- You must comply with all state or federal laws or regulations, including laws that apply to insurance practices (especially related to Medicaid and Medicare), government contracting/procurement, and employment.
- You must not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation, or unfair dealing.
- All company records, books, and accounts must be maintained in a fair and accurate manner. Falsification or modification of company records is prohibited.
- Destruction or modification of any document that could potentially be relevant to reasonably anticipated or pending litigation or investigation is prohibited.
- The making, acceptance, or approval of any inappropriate inducement such as a bribe, kickback, or other illegal payment is strictly prohibited.
- Do not solicit, accept, or use confidential information that was obtained improperly.
- You must notify HR immediately if you have been debarred, excluded, or suspended from working with any federally sponsored program (e.g. Medicaid or Medicare).
- You are prohibited from speaking on Meridian's behalf unless you have sought and received the prior approval of senior management or Meridian's Board of Directors, whether to a customer, member, contractor, vendor, or the media.
- No money paid to Meridian from a government contract may be used to influence or lobby for the award of any other government contract.

GIVING OR RECEIVING GIFTS

To avoid the implication that unfair or preferential treatment, any gifts, favors, and gratuities exchanged in the normal course of business must be appropriate. If you have any questions as to whether a gift, favor, or gratuity is appropriate, please contact your supervisor/contract administrator or HR. It is never permissible to give or accept expensive gifts or other benefits, especially gifts of cash, gift cards, or other cash equivalents. Inexpensive gifts, favors, and gratuities may be given or received only if they are consistent with accepted business practices and are of such limited value, defined as under $5, that they cannot be considered as a bribe or pay-off. If someone offers you an expensive or inappropriate gift, you are expected to politely refuse the gift and explain Meridian's policy regarding the acceptance of gifts.

Similarly, you are prohibited from accepting any preferential treatment offered to you as a result of your relationship with Meridian, including discounts, except for those corporate discounts which the company negotiates for all of its employees. For example, if you engage with a Meridian vendor for goods or services for your own personal purposes, you are expected to pay fair, market value for the good or service.

The offering of any gifts or benefits to anyone working for or representing a state, local, or the federal government may be unlawful. Accordingly, you are prohibited from offering or promising gifts of any value, even minor gifts, to any person who works for a federal, state, or local government or agency where such gifts could possibly influence their official duties. This prohibition includes paying for travel expenses, lodging, meals, and entertainment.

POLITICAL ACTIVITY AND CONTRIBUTIONS

Meridian resources may not be used in support of any candidate for state or local office, any ballot initiatives, referendums, or questions, or any other political activity. You may not use Meridian resources to contribute to any political cause or candidate without the prior written approval of Meridian's General Counsel.

INTERACTIONS WITH OUTSIDE PARTIES

Any contact with outside parties such as the media or a government agency is strictly controlled for the protection of both you and Meridian. Any such contact must conform to Meridian policies and applicable laws. Public statements made by anyone known to be affiliated with Meridian should be made carefully, and any suggestion that those comments are associated with Meridian must be avoided. Your personal views should be clearly separated from those of Meridian.

Communications made to outside parties on behalf of Meridian, such as certain e-mails, mailings, public speaking, presentations, and posts to social media should be reviewed by the Communications Department and Meridian's General Counsel, if appropriate, before they are made. This includes anything you might send to members, potential members, or providers.

Any requests for comment or questions from the media must be forwarded to the Communications Department to review and issue a response. If your job duties require you to routinely interact with the media on Meridian's behalf, you should strive to understand Meridian's official position on each matter and not disagree with the company's position in public.

If you are asked by a vendor or provider for a quote for a press release, or are asked for a recommendation of a product or service Meridian utilizes, send the request to the Communications Department. Only those specifically designated by Meridian are authorized to formulate and express Meridian's views on legislation, regulations, or government action. You should not use your affiliation with Meridian when you write or speak in a personal capacity about issues that may be related to Meridian business. This includes posting to social media or the Internet.

PROTECTING CONFIDENTIAL INFORMATION

Protection of member protected health information (PHI), confidential business information, and trade secrets is imperative and we must work hard to maintain confidentiality. You must protect member PHI and other confidential information from unauthorized or inappropriate access, use, or disclosure.

"Confidential information" includes any information collected, produced, or developed by or for Meridian or its business relations. It includes but is not limited to patient medical records/history, technological prototypes and data, scientific formulas and prototypes, research and development strategies, intellectual property, client/customer lists, contracts and legal documents, current or pending projects and proposals, marketing plans/information, financial data/information and compensation data. It also includes information owned or created by a third party that has been disclosed to Meridian in the course of its business operations and pursuant to a license or confidentiality agreement.

Member PHI and other confidential information

To keep member PHI and other confidential information safe, you must:

- Never discuss proprietary information with any person from outside Meridian or in any public place where it is possible you could be overheard. Public places can even be areas within Meridian's office space, including restrooms, elevators, or break rooms.
- Never view, access, or distribute confidential information or PHI internally outside of authorized job duties or other appropriate business reasons.
- Never share or disclose confidential information or PHI with anyone outside of Meridian unless explicitly approved by Meridian's General Counsel or the Compliance Officer, depending on the circumstances. Disclosure must only be made pursuant to the law and for legitimate business purposes.
- Encrypt and send secure any e-mail communications containing PHI or confidential information that may be sent outside of Meridian's internal computer systems and otherwise comply with applicable Meridian electronic security standards and safeguards.
- Turn over paper documents containing member PHI or confidential information when they are not in use. Such documents should be locked up in a secure area at the end of your shift.
- Utilize the secure shredder bins to dispose of member PHI or confidential information properly.
- Place copyright notices on all materials created by Meridian intended for external or wide internal use. Consult with the Communications Department for the proper format of any copyright notices.
- Prevent the use of Meridian's intellectual property, including trademarks and copyrighted works, by anyone outside of Meridian unless permissible under an explicit license or confidentiality agreement approved by Meridian's General Counsel. If you become aware of any outside use of Meridian's intellectual property, report it immediately.

ENDING YOUR EMPLOYMENT OR OTHER RELATIONSHIP WITH MERIDIAN

All covered persons and FDRs are required to sign a Confidentiality Agreement as a condition of employment/contract/placement and should you leave Meridian for any reason, the obligation not to disclose member PHI and other proprietary information of Meridian and its customers continues. You are obligated to return any and all confidential information or PHI upon the end of your employment or other relationship with Meridian. Materials containing such information are not to be kept or otherwise removed from Meridian property. Meridian retains the right to inspect any property you have upon your departure to monitor for inappropriate removal of company information. If you have signed a confidentiality or other agreement with Meridian that extends for a time period beyond the end of your employment, you must continue to abide by the applicable terms of such agreement(s).

INSIDER TRADING

While Meridian itself is not a publicly traded company, it maintains business relationships with companies that are publicly traded. Laws and regulations regarding the trading of securities may apply to such companies. Through your relationship with Meridian, you may have access to confidential information about other companies. Some of this information may be considered "material, nonpublic information". You must not trade the securities of companies if you possess "material, nonpublic information" about them.

What is "insider trading"?

Insider trading refers to the illegal practice of buying or selling securities while possessing material, nonpublic information. Under U.S. federal or other local securities laws, it can also be illegal to tell or "tip" others to the "material, nonpublic information".

What is "material, nonpublic information"?

"Material, nonpublic information" is information that an investor would think is important when making a decision about buying, holding or selling a company's securities which has not been disclosed to the general marketplace.

Here are some examples:

- Annual or quarterly financial results or expected results
- Gain or loss of a major customer
- Negotiation or termination of major contracts
- Possible mergers or acquisitions
- New products, discoveries or services
- Changes in management
- Major litigation, litigation developments, or potential claims

The "material" or "nonpublic" nature of information may vary with the circumstances. Generally, information that would affect the price of a company's stock is "material". Information reported in press releases and public filings with the Securities Exchange Commission is public information. Information disclosed on a conference call, in an email, or to a handful of investment analysts may still be "nonpublic" information.

Meridian employees and FDRs are required to follow all applicable securities laws, including prohibitions on insider trading. Employees and FDRs should use the utmost discretion when discussing work or business matters with friends or family. Insider trading is illegal and may result in civil penalties or criminal prosecution.

Complying with insider trading rules

You are expected to:

- Refrain from trading a company's securities if you have "material, nonpublic information" concerning that company's business operations or financial condition such that the trade would violate Securities and Exchange Commission rules.
- Limit any trading in a company's securities until it is reasonable to think that all information material to your decision is public.
- Refrain from disclosing or discussing any material, nonpublic information regarding about another company with anyone inside or outside of Meridian unless necessary to your job functions, Meridian's business operations, and/or pursuant to the express approval of Corporate Legal Counsel.

You do not have to personally profit from the inappropriate use of material, nonpublic information in order for it to be unethical and illegal. Complying with these rules will protect both you and Meridian.

FRAUD, WASTE, AND ABUSE (FWA)

Meridian takes FWA cases seriously and has established procedures to prevent, detect, and report allegations of FWA. Meridian encourages you to report any knowledge or suspicion of any act or practice which may constitute FWA to the appropriate staff.

What is "fraud"?

Fraud is an intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to himself or some other person. It includes any act that constitutes fraud under applicable state or federal law.

What is "waste"?

Waste involves the overutilization of services, misuse of resources, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare or Medicaid Program. Waste relates primarily to mismanagement, inappropriate actions and inadequate oversight.

What is "abuse"?

Abuse means practices that are inconsistent with sound fiscal, business, or medical practices, and result in an unnecessary cost to the Medicaid, Medicare and Commercial programs, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care.

Here are some examples of FWA:

- Billing more than once for the same service (i.e., double billing)
- Billing for services never performed or medical equipment/supplies never ordered/delivered
- Performing inappropriate or unnecessary services
- Providing lower cost or used equipment while billing for higher cost or new equipment
- Using someone else's identity
- Attempting to fill an altered or false pharmacy prescription
- Giving false information to receive medical or pharmacy services
- Selling member ID numbers
- Setting up invalid provider records and diverting payments to the employee or someone else
- Falsifying provider credentials
- Forging or altering prescriptions
- Promoting underutilization through denials of services
- Receiving illegal payments or other benefits to prescribe certain medications
- Dispensing expired or adulterated prescription drugs

You are required to receive FWA training upon initial hire/contract and annually thereafter. If you suspect FWA involving Meridian or its members, providers, contractors or any other affiliate of Meridian, you should report it immediately to your supervisor/contract administrator. You may also report directly to the Compliance Officer and/or the state or federal government. Reports may be made anonymously if you choose.

COMPLIANCE WITH FEDERAL & STATE LAWS

You must comply with certain federal and state laws, statutes and requirements that govern all our businesses, including Commercial, Medicare and Medicaid.

ENFORCEMENT

Meridian strictly enforces this Standards of Conduct. All covered persons are subject to discipline, including termination of employment/contract, for noncompliance. Noncompliance includes, but is not limited to:

- Failure to follow this Standards of Conduct or other Meridian policies
- Failure to follow any state or federal laws or regulations that apply to Meridian
- Asking another employee to violate this Standards of Conduct or any state or federal law or regulation
- Failure to report violations or any state or federal law or regulation, including leaders who fail to recognize and act upon a violation
- Concealing a violation or obstructing an investigation
- Engaging in retaliation against an employee who has reported a suspected violation

MAINTENANCE

This document is updated at least annually and can be located on the Medicare Compliance Department website. Any changes to this document will be promptly redistributed.

REPORTING CHANNELS

INTERNAL	Senior Vice President, Medicare & HIX Compliance Officer 1 Campus Martius Detroit, MI 48226
	Vice President of Regulatory Compliance and Accreditation 1 Campus Martius Detroit, MI 48226
	Anonymous EthicsPoint FWA Hotline http://mhplan.ethicspoint.com/ 1-855-375-6725
FEDERAL	**Centers for Medicare & Medicaid Services** Office of Inspector General Attn: OIG Hotline Operations P.O. Box 23489 Washington, DC 20026
STATE	**State of Michigan-Office of Inspector General** PO Box 30479 Lansing, MI 48909 855-MI-FRAUD www.michigan.gov/fraud
	Illinois State Police -Medicaid Fraud Control Unit 801 South Seventh St, Suite 500 – A P.O. Box 19461 Springfield, IL 62794 888-557-9503
	Ohio Department of Insurance-Fraud Unit 50 W. Town Street, Third Floor – Suite 300 Columbus, OH 43215 800-686-1527 614-387-0092 (fax) ODI.Fraud@insurance.ohio.gov
	Indiana Department of Insurance-Consumer Services Division 311 West Washington Street Indianapolis, IN 46204-2787 800-622-4461 317-234-2103 (fax) http://www.in.gov/idoi/2547.htm#6
	State of Kentucky-Cabinet for Health and Family Services Office of the Inspector General-Division of Audits and Investigations 275 East Main Street, 5 E-D Frankfort, KY 40621 800-372-2970 502-564-7876 (fax)

FAQ

If I am aware of a potential compliance or FWA issue, do I have an obligation to report it?

Yes. Not only is it our policy to require you to report all potential issues of noncompliance and FWA, but government regulations require it as well.

Can I get in trouble for making a good faith report?

No. Our policy protects you from being retaliated against for making a good faith report of a potential compliance or FWA issue. In addition, government regulations prohibit anyone from retaliating against you in the same manner.

What are some examples of compliance or FWA issues that should be reported?

- **Bid:** Overstating or understating bid data to obtain higher premiums from members or higher reimbursement from the government.
- **Call center:** Providing beneficiaries with inaccurate information.
- **Claims:** Submitting claims to the government for services that were never rendered, failure to pay providers at the correct rate, paying providers who are on the Medicare opt-out or OIG exclusion list, inappropriately denying member and provider claims.
- **Enrollment and disenrollment:** Improperly enrolling members to obtain higher reimbursement from the government, improperly disenrolling members due to high medical expenses or other medically-related reasons.
- **Exceptions and appeals:** Not approving members for medically necessary services.
- **Health services:** Failing to approve members for medically necessary services.
- **Premium billing:** Billing members at the incorrect premium amount, not providing members with the required grace period to pay their bills.
- **Pharmacy:** Denying members their transition supply, applying utilization management rules that have not been approved, inappropriately denying drugs that are should be covered.
- **Provider network:** Not credentialing providers in accordance with credentialing laws and regulations, contracting with providers who are on the Medicare opt-out or OIG exclusion list.
- **Sales and marketing:** Misleading beneficiaries, violating a CMS marketing rule, allowing agents and brokers to conduct illegal marketing activities.

This is not an exhaustive list. You may contact the Compliance Department further guidance. Remember, it is always better to over-report than under-report.

Do I have to do any investigation or extensive research before reporting an issue?

No. As long as you have a reasonable basis for believing a compliance issue has occurred, once reported, we will do the fact finding and investigation.

Will I be notified of the outcome of an issue I reported?

All efforts will be made to notify you of the outcome. Due to confidentiality reasons, you may not always be notified of the outcome. Rest assure, however, that your issue will be thoroughly investigated.

How often is the Compliance and FWA Program updated?

We are constantly reviewing and making enhancements to our program on a routine basis to meet changing business and regulatory needs. At a minimum, the Compliance and FWA Program is updated annually.

What is the difference between the "Compliance Program" and the "Standards of Conduct"?

The Standards of Conduct is a subset of the Compliance Program, and addresses personnel matters such as ethical behavior, conflict of interest and gifts. The Compliance Program is the larger, more global infrastructure by which activities are governed.

Is the Compliance Department only to be contacted when there is an issue?

No. We encourage you to openly ask questions, seek a regulatory interpretation, or go over an issue of fact that you are unsure about.

Will results from monitoring and auditing activities be shared with government agencies?

We sometimes disclose issues to the government results from our monitoring and auditing activities, depending on the risk and severity of the findings.

What is the difference between a "compliance" issue and a "fraud, waste and abuse" issue?

Fraud, waste and abuse issues are types of compliance issues, and usually involve a financial or monetary impact to the government and tax payers.

Is an FWA issue more severe than a compliance issue?

No. The severity of the issue will depend on the facts and circumstances.

Where can I get more information on compliance?

You are always encouraged to contact the Medicare Compliance Department, or visit us at: https://share13.mhplan.com/sites/compliance/medicarecompliance/SitePages/Home.aspx.

REFERENCES

Compliance Department: Provides comprehensive information on Meridian Health Plan's Compliance Program.

Medicare Fraud Strike Force: Provides news and updates on national health care fraud, including tips on how to protect against fraud.

Office of Inspector General: Provides news and updates on national health care fraud, including law enforcement actions taken against fraudulent parties.

US Department of Justice: Provides news and updates on national health care fraud.

Medicaid Anti-Fraud: Provides information on Medicaid fraud.

Effective Date	January 1, 2017
Approval Date	December 20, 2016 (Medicare & HIX Compliance Committee)
Revision Date	December 2016
Line(s) of Business	Medicare & HIX (compliance policies) All (Standards of Conduct)
Department Owner	Medicare & HIX Compliance