# DME CONSULTING GROUP

## Compliance Policies Handbook

**TABLE OF CONTENTS**


COMPLIANCE PROGRAM OVERVIEW ..... 1

1. Introduction ..... 1

2. DME-CG Committee ..... 1

3. Who does this program apply to? ..... 1

4. Our expectations ..... 2

5. Dissemination ..... 2

6. DME-CG's ethical principles ..... 2

7. Compliance Program in brief ..... 3

DME-CG POLICIES ..... 7

Policy #1: Compliance with Federal and State Laws ..... 7

Policy #2: Compliance Officer, Compliance Committee and Governing Body ..... 11

Policy #3: Compliance Training and Education ..... 18

Policy #4: Effective Lines of Compliance Communication, Reporting & Non-Retaliation ..... 21

Policy #5: Personnel Corrective Actions ..... 27

Policy #6: Compliance Monitoring and Auditing ..... 34

Policy #6A: Exclusion and Background Check ..... 37

Policy #7: Compliance Investigation & Corrective Action Plan ..... 41

Standards of Conduct ..... 55

# I. COMPLIANCE PROGRAM OVERVIEW

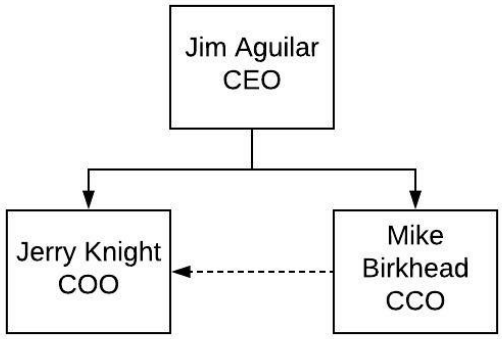
## Introduction

At DME-CG, we have a corporate responsibility of providing industry-leading services to our growing community of Health Plan providers and their member base. We 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 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.

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 our Staff and Clinical Consultants for their continued support in our ongoing commitment to serve our clients in the best and most ethical manner.

### DME-CG Committee




| DME Consulting Group Compliance Committee Contact Information | | | |
|---|---|---|---|
| Jim Aguilar | Chief Executive Officer | (707) 474-2380 | jim@dme-cg.com |
| Jerry Knight | Chief Operations Officer | (770) 335-1656 | jerry@dme-cg.com |
| Michael Birkhead | Chief Compliance Officer | (415) 722-0552 | compliance@dme-cg.com |

### Who does the Compliance program apply to?

This Compliance and Fraud, Waste and Abuse (FWA) Program applies to all DME-CG

Management team, Staff members, Clinical Consultants, and members of the Board of Directors.

## Our expectations

All Staff members, Clinical Consultants and Board of Director members are required to read and be familiar with the Compliance and FWA Program at the time of hire, appointment or contractual engagement, and annually thereafter. All must learn to recognize potential noncompliant and FWA issues that may arise during the course of carrying out work duties and report them to the appropriate channel and assist in remediating them. All are obligated to improve each department's process to minimize compliance risks to DME-CG, our clients and our State and Federal regulatory agencies. Ultimately, all are strongly encouraged to be champions and advocates 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:** The Head of Administration will disseminate the Compliance and FWA Program, including the Code of Business Conduct and Ethics, to new staff and directors during onboarding process and prior to officially starting work. All employees, staff and directors are required to sign an acknowledgment and agreement.

**Annually:** The Head of Administration will disseminate the Compliance and FWA Program, including the Code of Business Conduct and Ethics, to employees, staff and directors **annually** thereafter, and after material updates.

**FDR:** The Chief Compliance Officer will disseminate the Compliance and FWA Program and Code of Business Conduct and Ethics to applicable FDRs during initial process of contracting. The Chief of Compliance disseminates the document to the FDRs **annually** thereafter, using various dissemination methods, including:

- Broadcast of electronic copies
- Posting on company intranet

## DME-CG's ethical principles

- Full compliance with both the letter and spirit of the law.
- Delivery of high-quality DME Assessments and related services at fair prices which are

reasonable and competitive.

- Conduct all our relationships with integrity, objectivity and accountability.
- Pursue financial responsibility, stability and growth, delivering a quality of earnings that meet the highest standards of legal and fiscal principles.
- Be a positive influence and good corporate citizen in the communities where DME-CG provides services.
- Develop mutually beneficial partnerships with competitors, payers, and other providers of health care services, placing the good health of the community above personal or corporate gain.
- Treat Staff members, customers and competitors fairly and with respect.
- Report to DME-CG officials illegal or unethical practices of DME-CG Staff members or Clinical Consultants.

These Ethical Principles are not a moral judgment or a license to dictate the religious, political, or personal preferences of our fellow Staff members. Rather, these Principles are the bedrock of professional and personal standards on which we anchor our business decisions and relationships. These Ethical Principles are founded in the time-honored tenets of being honest, loyal, industrious, fair, responsible, reliable and of service to others.

DME-CG's Ethical Principles are a blueprint for living and decision-making in the business environment but are not a substitute for following DME-CG's other policies, procedures and practices either set forth elsewhere in this Manual or elsewhere in DME-CG's other policies. Any questions about DME-CG's Ethical Principles or other ethical concerns, can be discussed with a supervisor if appropriate or can be directed to the DME-CG Chief Compliance Officer.

## Compliance Program in brief

The Compliance Program and the content contained herein are a collection of incorporated policies, procedures, and guidance by which our Medicare program is 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 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.

## Definitions

**Abuse** includes actions that may, directly or indirectly, result in: unnecessary costs to the Medicare Program, improper payment, payment for services that fail to meet professionally recognized standards of care, or services that are medically unnecessary. Abuse involves payment for items or services when there is no legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment. Abuse cannot be differentiated categorically from fraud, because the distinction between "fraud" and "abuse" depends on specific facts and circumstances, intent and prior knowledge, and available evidence, among other factors.

**Compliance** is an act or process of complying with a demand or conformity in fulfilling official requirements.

**Contractor** is an individual to whom DME-CG has granted unique user identification so that

the person can use the company's computer network equipment and, by virtue of his or her user identification, gain access to the company's intranet, internet and other computer systems.

**Downstream Entity** is any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the Medicare Advantage or Prescription Drug benefit, below the level of the arrangement between a Medicare Advantage Organization or applicant or a Prescription Drug plan sponsor or applicant and a first-tier entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services. (See 42 C.F.R.§, 423.501).

**FDR** means First Tier, Downstream or Related Entity.

**First Tier Entity** is any party that enters into a written arrangement, acceptable to CMS, with a Medicare Advantage Organization or Prescription Drug plan sponsor or applicant to provide administrative services or health care services to a Medicare eligible individual under the Medicare Advantage program or Prescription Drug program. (See 42 C.F.R. § 423.501).

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

**FWA** means fraud, waste and abuse.

**GSA** means General Services Administration.

**HIPAA (Health Insurance Portability and Accountability Act)** is United States legislation (1966) that provides data privacy and security provisions for safeguarding medical information.

**HITECH - Health Information Technology for Economic and Clinical Health Act**, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.

**HITRUST- Health Information Trust Alliance**, is a privately held company located in the United States that, in collaboration with healthcare, technology and information security leaders, has established a Common Security Framework (CSF) that can be used by all organizations that create, access, store or exchange sensitive and/or regulated data. The CSF includes a prescriptive set of controls that seek to harmonize the requirements of multiple

regulations and standards.

**HPMS (Health Plan Management System)**. The Centers for Medicare & Medicaid Services (CMS) Health Plan Management System is a well-established information system that serves a critical role in the ongoing operations of the Medicare Advantage (MA) and Part D programs

**OIG** means the Office of the Inspector General within Department of Health and Human Services (DHHS). The Inspector General is responsible for audits, evaluations, investigations, and law enforcement efforts relating to DHHS programs and operations, including the Medicare program.

**Related Entity** is any entity that is related to a Medicare Advantage Organization or Prescription Drug plan sponsor by common ownership or control and performs some of the Medicare Advantage Organization or Prescription Drug plan sponsor's management functions under contract or delegation; furnishes services to Medicare enrollees under an oral or written agreement; or leases real property or sells materials to the Medicare Advantage Organization or Prescription Drug plan sponsor at a cost of more than $2,500 during a contract period. (See 42 C.F.R. §423.501).

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

# II. DME-CG POLICIES

## Policy #1: Compliance with Federal and State Laws

DME-CG will comply with applicable Federal and State laws and statutes, Code of Federal Regulations and sub-regulatory guidance.

## Requirements:

DME-CG 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, 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. DME-CG 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 DME-CG.

**Beneficiaries Inducement Statute:** Medicare marketing guidelines prohibit DME-CG 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:** DME-CG must comply with Federal regulations that implement and oversee the Medicare, HIX and security & privacy programs. These regulations include:

42 CFR §400: Overview42 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
HIPAA Administrative Simplification, Subpart E Privacy Rule
HIPAA Administrative Simplification, Subpart C Security Rule
HIPAA Administrative Simplification, Subpart D Data Breach Notification Rule
21 CFR Part 11
ISO/IEC 27001:2013

**Contractual Commitments:** DME-CG contracts with government agencies such as the Centers for Medicare and Medicaid Services (CMS), 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.

**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 DME-CG 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 DME-CG 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.

**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, DME-CG 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. DME-CG shall comply with such guidance.

# Policy #2: Compliance Officer, Compliance Committee and Governing Body

DME-CG Compliance Officer maintains oversight for Medicare reports. 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 monthly.

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 DME-CG'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.

## Requirements:

### Compliance Officer:

**Reporting & Accountability:** The Compliance Officer reports to and is directly accountable to 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.

**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 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 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 other internal and external audit departments, 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 the Head of Administration to ensure that covered persons are checked against the OIG exclusion lists and GSA debarment lists monthly. DME-CG 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 related lines 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: The Compliance Committee maintains memberships from a variety of backgrounds, including Physical Therapy, Health Services, Operations, IT, and Business Development and 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 the Compliance Committee at any time, following a formal request by at least one committee member. 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.
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 any 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 DME-CG doing to prevent issues from occurring?
- What is DME-CG doing to ensure compliance improvement from year-to-year?
- How is DME-CG performing relative to CMS expectations, the competitors, and the industry as a whole?

CEO and Executive Leadership Engagement

The CEO of DME-CG 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.

## Policy #3: Compliance Training and Education

DME-CG 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.

**Requirements:**

### General Compliance Training:

**Compliance Department:** Creates general and FWA training content for all covered persons; administers training to Board of Directors, and committee members 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 Resources:** Administers general and FWA training to employees; maintains 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.

### Compliance Training Schedule:

Employees & Consultants: Precondition for employment or within **30 days** of hire, and annually thereafter as a condition of employment.

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

- 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.

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 Training**:

- 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

# Policy #4: Effective Lines of Compliance Communication, Reporting & Non-Retaliation

## Effective Lines of Communication:

DME-CG 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, DME-CG maintains a non-intimidation and non-retaliation environment that allows individuals to make good faith reports against any person or action by DME-CG 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.

---

## Requirements:

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

2. Memos are classified based on:

   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.

   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 department heads 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 department heads 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. The department heads 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 to 14 business days**.

5. Once all necessary actions have been taken, the department head 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.

6. If the department head's comments are incomplete, we will work with the department head to ensure all appropriate actions are taken and documented properly.

7. Compliance will conduct follow-up outreach for memos marked as 'Follow-Up Needed'.

8. Non-responses will follow the escalation procedure:

9. 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.

10. On a **bi-weekly** basis, Compliance will review all outstanding notices to ensure appropriate and complete actions have been taken.

11. The Compliance Department will participate in operational meetings to provide oversight of complex or high-risk issues. Department heads are also encouraged to request the Compliance Department participate in other operational meetings during implementation.

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

**CMS Educational Notices:** The Compliance Department routinely disseminates new compliance information to department heads 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.

**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.

## Reporting:

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:

- Coverage Determinations Appeals and Grievances (CDAG) and Organization Determinations Appeals and Grievances (ODAG)
  - Untimely effectuation
  - Inappropriate denials
  - Access to care issues
  - Member notice issues
  - Misclassification of cases
- Untimely or inaccurate Explanation of Benefits
- Call center
  - Not meeting performance standards
  - Inaccurate information provided
  - Downtime
- Enrollment & disenrollment
  - Untimely member notice
  - Inappropriate enrollment & disenrollment

## Method of Reporting

DME-CG 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 it using one of the methods outlined above
2. Report directly to your DME-CG contract administrator
3. Report to the DME-CG Compliance Officer
4. Report anonymously to compliance@dme-cg.com or (866) 298-7047

If you are a DME-CG vendor, in addition to any of the methods outlined above, you may report to your DME-CG 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 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 DME-CG's corrective action policy.

Furthermore, if you are filing a qui tam action under the Federal False Claims Act, also known as a type of whistleblower claim, 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 DME-CG's non-retaliation Policy will be subject to the disciplinary policy.

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.

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.

## Policy #5: Personnel Corrective Actions

DME-CG 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 DME-CG and its affiliated health plans' ability to meet contractual, statutory and other obligations. DME-CG's policy with respect to administering corrective actions is designed to ensure that employees whose performance or conduct does not meet DME-CG's standards are treated fairly and in a consistent manner. Employees whose performance or conduct does not meet DME-CG'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 DME-CG, 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 DME-CG's employment policies, procedures and manuals. These procedures do not create any contractual obligation on the part of DME-CG. The procedures are provided as a guideline for discipline in those situations where DME-CG, in its sole discretion, believes that such action is in the best interest of both DME-CG and the employee.

### Requirements:

**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 DME-CG. 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 Violation of Privacy and Security policies and procedures.

9. Violation or 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 DME-CG. 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 DME-CG Compliance policies, 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 Performance Improvement Program 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.

## Investigation

A thorough investigation must be conducted before disciplinary action is administered. Depending on the situation, the investigation may be conducted by Compliance Department. 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.

## 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 and the Compliance 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 DME-CG 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 DME-CG'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. 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.
    b. 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 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 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

DME-CG ensures that corrective action policies and actions are applied consistently by:

- Promptly addressing and responding to all inappropriate behavior and poor performance.
- 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

DME-CG requires all clinical consultants and employees to report and disclose any potential compliance, HIPAA or FWA issues. Clinical consultants and employee sare 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.

## Policy #6: Compliance Monitoring and Auditing

DME-CG 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.

### Requirements:

#### 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 an annual 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
- Department head 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
- Security and Privacy

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 department heads 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 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, department heads 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 department heads for correction If there is a continued pattern of deficiencies, Compliance will initiate a Corrective Action Plan.

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

## 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.

## Policy #6A: Exclusion and Background Check

**DME-CG does not** hire, contract with, or allow any individual who has been sanctioned or excluded from participating in Medicade to work in such programs.

All new and existing employees, board members and officers, and contractors are required to immediately disclose to DME-CG 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, DME-CG will conduct other background checks prior to an offer of employment, such as criminal records, driving records, and education and professional credentials.

DME-CG will not contract with any person or entity sanctioned or excluded from participating in Medicare or who have opted-out of the Medicare program.

In addition to completing an extensive background submission, all contracted individuals and companies are required to immediately disclose to DME-CG any debarment, exclusion or any other sanction event that makes them ineligible to perform work or receive payment for work related directly or indirectly to Federal health care programs.

---

### Requirements

### 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.

<u>At Time of Hire/Appointment</u>:

**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/public/SAM/. 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, DME-CG 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 DME-CG, 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 DME-CG 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 DME-CG 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.

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 DME-CG 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)
- 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 #7: Compliance Investigation & Corrective Action Plan

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

## Requirements

### 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
- HR exit interviews or questionnaire

To that end, DME-CG 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

DME-CG conducts data analysis through the use of data mining tools to prevent, detect, and correct noncompliance and FWA. We utilize 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

## 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:
   - U.S. Department of Justice
   - HHS Stop Medicare Fraud
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:
   - NPI Registry
   - Medicare Physician Lookup
   - OIG Exclusions List
   - Federation of State Medical Boards
   - Secretary of State website for your state
   - State licensing/medical board website
4. Verify the provider's contract status with Provider Network
   - If no match, retain screen print or document "no match" finding and follow Step 8.
   - 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:
   - Create impact analysis to claim dollar, member, and provider
   - Report all positive match findings to FWA Committee with action plan to recover/recoup, suspend/terminate provider, and other appropriate actions
   - The FWA Committee then follows its procedure
8. Provide monthly summary report to the Compliance Officer

## SIU & Fraud Committee

**Purpose:** DME-CG 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 Compliance Manager 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 Health Services, Technology, Human Resources, 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. Monitor fraudulent activity and take appropriate actions when necessary.

8. Prevent illegal activities.

9. Provide fraud awareness training to applicable individuals.

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

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

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

13. Make recommendation to suspend, sanction or terminate anyone violating documented policies.

## Referral, Disclosure & Coordination with External Agencies

DME-CG will refer matters over to Federal and State regulatory agencies and law enforcement 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

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

## 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.

## 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. DME-CG shall permit Federal and

State agencies to inspect, evaluate, or audit books, records, documents, files, accounts, and facilities maintained by or on behalf of DME-CG or by or on behalf of any FDR, as required to investigate an incident of fraud and abuse.

DME-CG shall cooperate, and requires its FDR to cooperate, with Federal and State investigators during any investigation of fraud or abuse.

In the event that DME-CG reports suspected fraud or abuse by an FDR, or learns of a Federal or State investigation of an FDR, DME-CG should not notify or otherwise advise its FDR of the investigation. Doing so may compromise the 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 Timelines 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 oriental 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:** Tracks where the CAP is in the 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:** 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.

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.

# Standards of Conduct

The DME Consulting Group, Inc. (DME-CG) values the contribution of all employees, Commissioners, Committee Members, and Contracted Business Partners toward the goal of providing the highest possible quality of services to its members and providers. This Code of Conduct is created in accordance with state and federal requirements to provide guidance in following the ethical, legal, regulatory, and procedural principles that are necessary for maintaining high standards. This document serves as a guide for complying with DME-CG's internal policies and procedures as well as all applicable laws and regulations.

This Code of Conduct, approved by the DME-CG Management, applies to all DME-CG staff, including employees, temporary staff and interns, as well as Commissioners, Committee Members, and Contracted Business Partners. In this document, the word employee encompasses all four groups unless otherwise stated.

The consequences for DME-CG organizationally of failing to comply with this Code of Conduct can be serious, including member, financial, and reputational harm. Failure to comply may result in disciplinary actions up to and including termination.

Although this document was designed to provide overall guidance, it does not address every situation. Please refer to DME-CG Policies and Procedures on DME-CG's Intranet or in DME- CG's Human Resources (HR) Policy Manual if additional direction is needed.

If there is no specific DME-CG policy, this Code of Conduct becomes the policy. If a policy conflicts with this Code of Conduct, the Code of Conduct takes precedence. Questions or issues regarding this document or a policy should be discussed first with the immediate supervisor. If additional guidance is needed, one should go through the chain of authority up to and including DME-CG's Chief Compliance Officer, Chief Operations Officer, or the Chief Executive Officer.

---

**Requirements**

## Introduction

The DME Consulting Group, Inc. (DME-CG), a privately held consulting company, provides in-home medical necessity evaluation services to local, regional, and national Managed Health Insurance Plans. Since 1997 our Mobility Benefit Management (MBM) program has provided Medical Management teams with a balanced approach to utilization, pricing, and workflow for

Medicaid, Medicare, commercial, and federal lines of business. The success of our MBM program is the result of our expertise, a robust network of state licensed physical and occupational therapists, a unique two-tiered medical necessity review process and a state-of-the-art technology platform that provides HIPAA, HITECH, and, HITRUST assurance and security. For these reasons we are able to deliver objective, in-home data necessary to accurately determine medical need and apply coverage criteria so medical management can confidently make benefit decisions.

The DME Consulting Group, Inc. improves the health of our members through high quality and preventive care.

We have a vision, that healthy is for everyone.

## Guiding Principles

- We advocate for the health care needs of our client's members and other underserved residents of the United States of America.
- We address the safety and mobility related challenges faced by patients and providers which place vulnerable individuals at risk.
- We give individual and personal attention to our client's members and provider network.
- We respond to the cultural and linguistic diversity of our members.
- We advocate for DME-CG providers by ensuring they receive timely payment for their services and by reducing administrative obstacles.
- We support the effective and efficient use of health care services.
- We strive for a positive work atmosphere that encourages employee growth and commitment to DME-CG's mission.

## Objectivity

At DME-CG, we push for objectivity, transparency, and expedience in all we do, every day, in every way, to bring a better quality of life to the people in our community. Whether it is advocating for expanded care for the underserved, improving processes clients, or providing personal assistance to their members—we believe that objectivity, transparency, and expedience benefits everyone.

This commitment is our daily focus. It's in how we serve our clients and their members. It's in the hearts and on the minds of each and every staff member.

## Commitments

This Code of Conduct is intended to help both the DME Consulting Group, Inc. as a whole and

individual employee stay true to the following commitments.

To DME-CG Members
DME-CG is committed to delivering quality, affordable health care by providing its members access to a network of credentialed health care providers, customer service staff, and a grievance and appeal process for timely problem resolution.

To DME-CG Providers
DME-CG is dedicated to providing efficient network management resources for its contracted providers, honoring contractual obligations, delivering quality health services, and bringing efficiency and cost-effectiveness to health care.

To DME-CG Community Partners
DME-CG is dedicated to advocating for consistency and objectivity in the administration of healthcare benefits and outcomes as they related to safety and mobility of medically vulnerable individuals.

To DME-CG Contracted Business Partners
DME-CG is committed to managing client relationships in a fair and reasonable manner. The selection of Contracted Business Partners, e.g. vendors, contractors, suppliers, and First- tier, Downstream, and Related entities (FDRs), is based on objective criteria including quality, technical excellence, price, delivery, adherence to schedules, service, and maintenance of adequate sources of staff and supply. Competitive procurement is encouraged. DME-CG will not communicate confidential information given to us by its suppliers unless directed to do so by the supplier or by law.

## Standards of Conduct

All DME-CG employees, Commissioners, Committee Members, and Contracted Business Partners are responsible for following these guidelines.

## Privacy and Confidentiality

- Respect the privacy of members, providers, and co-workers by safeguarding their information from physical damage, maintaining member health information and business documents in a safe and protected manner, and following DME-CG's record retention policies.
- Protect the privacy of DME-CG members' protected health information (PHI) according to federal and state requirements.
- When using, disclosing, or requesting PHI, limit the information to the minimum amount

needed to accomplish the work. Do not share or request more PHI than is necessary.

- Only share medical, business, or other confidential information when such release is supported by a legitimate clinical or business purpose and is in compliance with DME-CG policies and procedures, and applicable laws and regulations. Whenever it becomes necessary to share confidential information outside DME-CG for legitimate business purposes, release PHI only after obtaining a signed business associates' agreement, corporate written approval or a completed Authorization to Release Information Form.
- Exercise care to ensure that confidential information, such as salary, benefits, payroll, personnel files, and information on disciplinary matters is carefully maintained and managed.
- Do not discuss confidential member, provider, contractor, or employee information in any public area, such as elevators, hallways, stairwells, restrooms, lobbies, or eating areas.
- Do not divulge, copy, release, sell, loan, alter, or destroy any confidential information except as authorized for DME-CG business purposes or as required by law.

## Security of Electronic Information

- Practice good workstation security, which includes locking up offices and file cabinets; disposing of all paperwork in appropriate shredding receptacles; and covering all PHI or locking the computer if stepping away from the desk.
- Take appropriate and reasonable measures to protect against the loss or theft of electronic media (e.g., laptops, flash drives, CDs/DVDs, photocopier hard drives, etc.) and against unauthorized access to electronic media that may contain member protected health information. Maintain and monitor security, data back- up, and storage systems.
- Maintain computer passwords and access codes in a confidential and responsible manner. Only allow authorized persons to have access to computer systems and software on a "need-to-know" basis.
- Do not share passwords or allow access to information to anyone that doesn't already have access or without written approval from Compliance committee
- Transmit electronic confidential information securely in encrypted form.

## Workplace Conduct

- Since DME-CG is comprised of teleRespect the dignity of every employee, provider, member, and visitor while providing high-quality services and treating one another with respect and courtesy.
- Communicate openly and honestly and respond to one another in a timely manner. Share information and ask questions freely.

- Be civil and comply with existing policies about the treatment of colleagues, non-harassment, and respect in the workplace.
- Conduct DME-CG business with high standards of ethics, integrity, honesty, and responsibility, and act in a manner that enhances our standing in the community.
- Support and observe a workplace free of alcohol, drugs, smoking, harassment, and violence.
- Do not act in any way that will harm DME-CG.

## Use of Social Media

- Use social media responsibly, whether posting words, pictures, audio files, or other electronic content. Social media includes Facebook, Twitter, YouTube, interactive websites, interactive microsites, blogs, wikis, chat rooms, and other such interactive venues. These guidelines apply whether at home or on personal time at work.
- Do not engage in discussions on social media sites that are incompatible with DME-CG's public image.
- As an employee, when one's connection to DME-CG is apparent, make it clear that the posting is on behalf of the individual and not DME-CG. A disclaimer to social media posts or sites indicating this should be provided.
- Protect members' confidentiality and protected health information at all times. Do not write or say anything that violates DME-CG's privacy, security, or confidentiality policies. Never post any information that can be used to identify an DME-CG member's identity or health condition.
- Maintain the confidentiality of DME-CG business information and do not discuss this information on social media sites.
- Always seek official approval before posting an official statement about DME-CG. Only designated staff may speak on behalf of DME-CG.
- When expressing personal views, always use a personal email address rather than the DME-CG email address, if an DME-CG employee.

## Adhering to Laws and Regulations

- Follow all state and federal laws and regulations, including reporting requirements.
- Do not knowingly make any false or misleading statements, verbal or written, to government agencies, government officials or auditors.
- Do not conceal, destroy, or alter any documents.
- Do not give or receive any form of payment, kickback, or bribe or other inducements to members, providers, or others in an attempt to encourage the referral of members to use a particular facility, product, or service.

- Avoid inappropriate discussions regarding business issues.
- Safety Considerations
- Comply with established safety policies, standards, and training programs to prevent job-related hazards and ensure a safe environment for members, providers, employees, and visitors.
- Wear an DME-CG badge at all times while in DME-CG offices and when representing DME-CG offsite.

## Conflict of Interest

- Avoid actual, apparent, or potential conflicts between one's own interests and the interests of DME-CG. Comply with all legal requirements concerning conflicts of interest and incompatible activities. Complete all disclosure documentation as required.
- Act in the best interest of DME-CG whenever functioning as an agent of DME-CG in dealings with contractors, providers, members, or government agencies. This includes those acts formalized in written contracts as well as everyday business relationships with business partners, members, and government officials.
- As an DME-CG employee, do not directly or indirectly participate in, or have a significant interest in, any business that competes with or is a supplier to DME-CG. Only engage with a competitor or supplier if participation is disclosed to DME-CG in advance and agreed to in writing by the Chief Executive Officer (CEO). This guideline also applies to members of one's immediate family.
- As an DME-CG employee, do not engage in outside employment or self- employment that may conflict with the work of DME-CG. Adhere to DME-CG's Outside Employment/Self-Employment Policy, which can be found in the Human Resources Policy Manual.
- As an DME-CG employee, do not accept gifts and other benefits with a total value of more than $50.00 from any individuals, businesses, or organizations doing business with DME-CG.
- As an DME-CG employee, do not accept cash or cash equivalents (gift certificates, gift cards, checks or money orders) in any amount from any individuals, businesses, or organizations doing business with DME-CG.

## Protecting Assets

- Protect DME-CG's assets and the assets of others entrusted to DME-CG, including information and physical and intellectual property, against loss, theft, and misuse. Assets include money, equipment, office supplies, business contacts, provider and claims data, business strategies, financial reports, member utilization data, and data

systems.

- Take measures to prevent any unexpected loss or damage of equipment, supplies, materials, or services. Adhere to established policies regarding the disposal of DME-CG properties.
- Ensure the accuracy of all records and reports, including financial statements and reported hours worked.
- Report expenses consistent with and justified by job responsibilities. Adhere to established policies and procedures governing record management and comply with DME-CG's destruction policies and procedures.
- Do not modify, destroy, or remove electronic communications resources (e.g., computers, phones, fax machines, etc.) that are owned by DME-CG without proper authorization.
- Do not install or attach any mobile or remote devices or equipment to an DME-CG electronic communications resource without approval.
- Use DME-CG property and resources appropriately for the best interests of our members and DME-CG and in accordance with DME-CG's Acceptable Use Policy.
- Follow all laws regarding intellectual property, which includes patents, trademarks, marketing, and copyrights. Do not copy software unless it is specifically allowed in the license agreement and authorized.

## Participating in the Compliance Program

- Report any potential instances of fraud, waste or abuse or any suspected violations of the Code of Conduct or law to the Compliance Officer, one's immediate supervisor, Human Resource staff, or any DME-CG director. Concerns can also be reported anonymously through the Compliance Hotline.
- Cooperate fully with investigational efforts.
- Act in accordance with DME-CG's commitment to high standards of ethics and compliance.

## Employment Practices

- Conduct business with high standards of ethics, integrity, honesty, and responsibility. Act in a manner that enhances our standing in the community.
- Employ and contract with employees and business partners who have not been sanctioned by any regulatory agency and who are able to perform their designated responsibilities.
- Provide equal employment opportunities to prospective and current employees, based solely on merit, qualifications, and abilities.

- Do not discriminate in employment opportunities or practices on the basis of race, color, religion, sex, national origin, ancestry, age, physical or mental disability, sexual orientation, veteran status, or any other status protected by law.
- Conduct a thorough background check of employees and evaluate the results to assure that there is no indication that an employee may present a risk for DME- CG.
- Acts of retaliation or reprisal against any employee who in good faith reports suspected violations of law, regulations, DME-CG's Code of Conduct, or policies will not be tolerated.
- Provide an open-door communications policy and foster a work environment in which ethical and compliance concerns are welcomed and addressed to ensure that the highest quality of care and service is provided.
- Provide appropriate training and orientation so that employees can perform their duties and meet the needs of our members, providers, and the communities we serve.

## Resolving Issues and Concerns

- Protect the identity of people who call the Compliance Hotline, if they identify themselves, to the fullest extent possible or as permitted by law.
- Evaluate and respond to allegations of wrongdoing, concerns and/or inquiries made to the Compliance Hotline in an impartial manner. All allegations will be thoroughly investigated and verified before any action is taken.
- Take appropriate measures to identify operational vulnerabilities and to detect, prevent, and control fraud, waste, and abuse throughout the organization.
- Report, as appropriate, actual or suspected violations of law and policy to the state or federal oversight agency or to law enforcement.