Status **Active** PolicyStat ID **9656067**

Origination	02/2004	Owner	Lisa Artale Bross
Last Approved	06/2021	Document Area	All Lines of Business
Effective	06/2021	Applicability	Denver Health Medical Plan (DHMP)
Last Revised	06/2021	Document Types	Compliance, Policy
Next Review	06/2022		

Fraud, Waste, and Abuse

PURPOSE

To outline the measures taken by the Denver Health Medical Plan (DHMP) for detecting and preventing fraud, waste and abuse (FWA).

SCOPE

This policy applies to all DHHA employees assigned to DHMP ("DHMP Employees" or "DHMP Staff") and any other person or entity that performs an activity or function on behalf of DHMP, including physicians and other providers, subcontractors, vendors, consultants or agents.

DEFINITIONS

Abuse – Incidents or practices that are inconsistent with legal, ethical, accepted and sound business, fiscal or medical practices that result in unnecessary cost to health programs, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care.

Colorado Medicaid Fraud Control Unit (MFCU) – an entity within the Colorado State Attorney General's Office whose mission is to mitigate the risk of and support accountability for fraud, waste and abuse of state and federal Medicaid funds by individuals or companies.

Current Procedural Terminology (CPT) – Procedure codes developed by the American Medical Association utilized for coding claims. A numeric code(s) submitted to denote the actual services performed by the provider when treating a patient.

Fraud – An intentional deception or misrepresentation made by a person with the knowledge that the

deception could result in some unauthorized benefit to themselves or some other person. It includes any act that constitutes fraud under applicable Federal or State law.

Healthcare Common Procedure Coding System (HCPCS) – Standardized code system necessary for medical providers to submit health care claims to Medicare and other health insurances. HCPCS codes are based on the CPT code to provide standardized coding.

Identity Theft – A type of fraud that occurs when someone steals the personal information (like name, Social Security number, Medicaid/Medicare number, etc.) to obtain medical care, buy drugs, or submit false billings to a health insurer in another person's name.

Pharmacy Benefit Manager (PBM) – A company that contracts with health plans to provide prescription benefits to members through network pharmacies.

Special Investigations Unit (SIU) - An internal investigation unit responsible for conducting investigations of potential FWA.

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

POLICY

DHMP cultivates an understanding of, and maintains compliance with, relevant federal, state, and local laws, regulations and standards as outlined in this document and the Denver Health and Hospital Authority (DHHA) False Claims, Fraud, Waste and Abuse, Human Resources (HR) Principle and Practice.

To ensure compliance with federal and state false claims laws, DHMP has implemented procedures to detect and prevent FWA, and also supports the efforts of federal and state authorities in identifying incidents of fraud and abuse.

DHMP provides information to all DHMP employees, affiliates, vendors, consultants and agents about the Federal and Colorado false claims laws in place and the obligation to prevent and detect FWA in accordance with applicable laws and regulations.

PROCEDURES

A. **DHMP Policies and Procedures for Detecting and Preventing FWA**
DHMP has established policies and procedures intended to detect and prevent fraud, waste and abuse in state and federal health care programs as contained herein and is supported by additional policies as described below.

    1. The DHMP Provider/Vendor/Subcontractor Overpayments Policy is available in PolicyStat and provides a process framework for the identification, investigation, recovery, and reporting of provider, vendor, and subcontractor overpayment to ensure financial integrity, regulatory and contractual compliance.

    2. The DHHA Code of Conduct (“Code of Conduct”) is available in PolicyStat and addresses

the responsibilities for ensuring the accuracy of claims for reimbursement in the section entitled "Ensure Integrity in Financial and Billing Matters". Pursuant to the Code of Conduct, each employee has an obligation and responsibility to report any activity that appears to violate applicable laws, rules, regulations, or the Code of Conduct.

3. The Denver Health Enterprise Compliance Program ("Compliance Program") is available in PolicyStat and outlines the structure of the Compliance Program that helps the organization mitigate financial exposure to non-compliance with FWA regulations and policies. The Compliance Program contains the following elements for reducing risk:

    a. Designation of a Compliance Officer, Compliance Committee and high level oversight;

    b. Code of Conduct and compliance policies and procedures;

    c. Education and training;

    d. Open lines of communication and reporting;

    e. Responding to reported concerns;

    f. Auditing and monitoring;

    g. Enforcing standards and policies;

    h. Corrective action; and

    i. Institutional obligations concerning compliance.

4. The False Claims, Fraud, Waste and Abuse, HR Principle and Practice provides information for employees and non-employees regarding the applicable fraud and abuse laws and the expectation for identifying and reporting FWA.

5. The Non-Retaliation, HR Principle and Practice also addresses procedures for internal reporting and whistleblower protection. Pursuant to this Principle and Practice, DHHA prohibits retaliation against any employee of DHMP who intends to or has reported, in good faith, his/her concern about actual or potential unethical or illegal behavior including violations of government rules/regulations and the law.

B. **Awareness and Training**

DHMP takes a proactive approach to anti-fraud and abuse efforts through education and training programs designed to promote understanding of how fraud and abuse is defined, how fraud and abuse may be committed, how to identify suspected incidents of fraud and abuse, and reporting procedures when fraud or abuse is suspected. New and annual employee compliance and FWA training requirements are summarized in the Compliance Program.

Network Providers receive information with respect to the identification of fraud, waste and abuse, as well as the penalties for fraud, waste and abuse. This information is included in the Provider Agreement and/or Provider Manual. Fraud updates may also be included periodically in provider newsletters. Subcontractors and vendors are informed of DHMP's commitment to compliance and FWA detection and prevention through the dissemination of this policy, its First Tier, Downstream,

and Related Entity (FDR)/Subcontractor Compliance Guide, the Code of Conduct, and Compliance Program.

Members may be informed of information with respect to the identification of fraud, waste and abuse via member materials and information contained on the DHMP website. Fraud updates may be included periodically in the Member Newsletter.

C. **Identification**

1. Various types of fraud for DHMP staff to be aware of and identify include, but are not limited to:

    a. *Health Plan Fraud:* Fraud committed by DHMP is defined as acts committed through deception, misrepresentation or concealment by DHMP's employees and/or as directed by leadership of DHMP. Such acts may include failure to provide medically necessary services, marketing schemes, improper bid submissions, payments for excluded drugs, multiple billing, inappropriate formulary decisions, inappropriate enrollment/disenrollment, false information, and inaccurate data submission.

    b. *Fraud by Agents/Brokers* - Fraud committed by agents/brokers is defined as deception, misrepresentation or concealment by a licensed representative to obtain something of value for which he/she would not otherwise be entitled. Examples of agent/broker fraud may include enrolling a group of individuals to form a nonexistent company; falsifying location of a group to gain insurance or obtain lower premium rates; adding false individuals to the group to avoid being medically underwritten; and/or false advertising.

    c. *Fraud Due to Misrepresentation of Enrollment Information* - Fraud due to misrepresentation of enrollment information is defined as commission of an act of deception, misrepresentation or concealment, or allowing it to be done by someone else, to obtain coverage for which one would not otherwise be entitled. Examples of eligibility fraud may include individuals joining to form a nonexistent group for insurance purposes; dependents not meeting the definition of a dependent (e.g., a significant other, grandchildren or a child who is not a full-time student); and/or not disclosing medical conditions on an application, where applicable.

    d. *Claims Fraud* – Examples of indicators include but are not limited to: provider is not in the insured's geographic region, member is in a different state than DHMP and no group affiliations exist for that state, large bills incurred just prior to term date or immediately after effective date, inconsistencies in company information versus medical records.

    e. *Provider Fraud* -Provider fraud is defined as "the devising of any scheme by any provider of health care or services to defraud for the purpose of personal or financial gain by means of false or fraudulent pretenses, representations, or promises." Examples of provider fraud may include: Billing for services not rendered; Providing "free" services and billing the insurance company (Providers must use correct billing codes, even though a service may not be

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

f. *Dental Fraud*: Examples of dental fraud may include: Billing for dental services not rendered; Providing excessive dental work that is not needed by the patient; Falsifying the date of service to correspond with the member's coverage period; Billing for non-covered services using an incorrect code (Current Dental Terminology (CDT) and/or diagnosis codes) to have the services covered.

g. *Pharmacy Fraud* - Lack of integrity of data to establish payment and/or determine reimbursement. Pharmacies may not reward health care providers for writing prescriptions for drugs or products. Examples of pharmacy fraud may include: Providing less than the billed quantity of a drug to a member; Billing for brand when generic drugs are dispensed; Billing multiple payors for the same prescriptions; Dispensing expired or adulterated prescription drugs; Forging or altering prescriptions; Refilling prescriptions in error.

h. *Pharmacy Benefit Management Fraud* – Examples may include: Unwarranted therapeutic substitution; Unlawful remuneration; Prescription drug shorting; Failure to offer negotiated prices.

i. *Pharmacy Wholesale Fraud* – Examples may include: Inappropriate documentation of pricing information; Speculative buying; Counterfeit and adulterated drugs through black market purchases.

j. *Pharmaceutical Manufacturer Fraud* - Examples may include: Kickbacks, inducements and other illegal remuneration; inappropriate relationships with physicians; Illegal usage of free samples.

k. *Member Fraud* - Member fraud is defined as the commission of acts of deception, misrepresentation or concealment by any policyholder or group of policyholders in order to obtain something of value to which they would not otherwise be entitled. Examples of member fraud may include: Alteration of bills, submission of false claims, applying for insurance when you know you are not eligible, member knowingly furnishes incorrect or incomplete information on applications, questionnaires, forms or statements, reselling drugs on the black market, doctor shopping, identity theft, forging or altering prescriptions, prescription stockpiling, improper coordination of benefits, failure to disclose information on applications, accident inquiries, coordination of benefits (COB) and full-time student information requests, etc.

l. *Vendor/Subcontractor Fraud* – Examples may include: Billing for services not rendered (e.g. for transportation, billing for trips/rides not given), providing excessive voucher trips above what is authorized by the plan, falsifying the

date of service to correspond with the member's trip, falsifying the plan approved pick-up destination and drop-off destination for transportation services

D. **Reporting Required**
The Code of Conduct and the Compliance Program provide all DHMP employees, affiliates, vendors, consultants and agents with a procedure for reporting integrity concerns regarding a violation of any law, regulation, and/or DHMP policy and procedure or Code of Conduct standards, including FWA. Reports may be made confidentially or anonymously. DHMP will protect individuals from being known within the limits of the law.

E. **Good Faith Reporting Protected**
As outlined in the Non-Retaliation, HR Principle and Practice and the Compliance Program, DHMP strictly prohibits retaliation against any DHMP employee, health care professional, subcontractor, or vendor who, in good faith, reports an actual or possible violation of any federal or state law or regulation, policy or ethical standard. All individuals are expected to cooperate fully in any investigation of an alleged violation. Additionally, our non-retaliation policy does not provide immunity for individuals who voluntarily disclose their own fraud, waste and abuse; however, self-disclosure may constitute a mitigating circumstance as to the penalties or discipline, if any, assessed or imposed.

F. **Reporting to Regulatory Agencies and/or Law Enforcement and Information Sharing**

1. The DHHA Chief Compliance and Audit Officer (CCAO), or designee, in collaboration with the Office of General Counsel, is responsible for the coordination of referrals to appropriate law enforcement and government authorities. Enterprise Compliance Services (ECS) works with the appropriate departments within DHMP to provide the maximum possible assistance to law enforcement and government agencies, in compliance with state and federal laws.

2. ECS may report instances of FWA for all products and lines of business, including medical, dental, pharmacy, commercial, Medicare Advantage, Medicaid, and CHP+.

3. With respect to DHMP's Medicaid line of business, DHMP will immediately report known confirmed intentional incidents of fraud and abuse to the Colorado Department of Health Care Policy and Finance's (HCPF) Contract Manager and to the appropriate law enforcement agency, including, but not limited to, the Colorado Medicaid Fraud Control Unit (MFCU). Additionally, DHMP will report indications or suspicions of fraud by giving a verbal report to the HCPF Contract Manager. DHMP shall investigate its suspicions and shall submit its written findings and concerns to the Contract Manager within three business days of the verbal report. If the investigation is not complete within three business days, DHMP shall continue to investigate. A final report shall be submitted within fifteen business days of the verbal report. The HCPF Contract Manager may approve an extension of time in which to complete the final report upon a showing of good cause. Additionally, DHMP reserves the right to suspend any payments to any participating or non-participating provider against whom there is a credible allegation of fraud at HCPF's or any other regulatory agency's request, with HCPF's or any other regulatory agency's approval, or when a matter is under active investigation for a credible allegation. Overpayments not suspected of being intentional instances of fraud and

abuse are also reported to regulatory agencies as outlined in the DHMP Provider/Vendor/ Subcontractor Overpayments Policy.

G. **Fraud Detection and Prevention**

1. Auditing, Monitoring and Risk Assessment

    a. The Compliance Program outlines the system DHMP has in place to ensure effective monitoring and auditing is conducted on a regular basis to test and confirm compliance with internal policies and procedures and federal, state and local laws and regulations governing its operations and to prevent, detect and correct actual or potential fraud, waste and abuse. This system includes an annual risk assessment, a risk-based monitoring and auditing work plan, and a mechanism to ensure corrective actions are taken when appropriate.

2. DHMP Claims Special Investigations Unit (SIU)

    a. The CCAO, or designee, is responsible for oversight of the SIU activities, including those of the vendor assigned to assist in fraud investigation efforts and the annual and ongoing reporting obligations of the SIU.

    b. DHMP utilizes internal personnel from its Payment Integrity Unit for SIU management that employs data-mining technologies, system driven analytics, algorithms, rules, and edits that assist in fraud identification efforts.

    c. Detection, prevention, and investigative activities are primarily conducted using the software tool created by DHMP, which is used for data analysis, querying, and reporting possible fraudulent and aberrant patterns from a combined database of DHMP's provider, member, claims, and pharmacy data. The software is a rules-based system that comes with built in FWA queries and reports (both standard and user-defined) to assist in the identification of suspicious trends and patterns.

    d. DHMP employs seasoned FWA experts across a wide variety of disciplines and has staff dedicated to DHMP's SIU activities. Other vendor resources are utilized for investigation and notification when appropriate. Additional external resources are contracted to supply specific case expertise when needed.

3. DHMP PBM SIU

    a. DHMP contracts with a PBM which conducts surveillance and investigations to detect and prevent potential fraud specific to DHMP's prescription drug benefit.

    b. The PBM is managed by DHMP's Pharmacy department.
    The PBM primarily uses the following methods to assist in fraud detection and prevention:

        i. Credentialing: Prior to participation in the PBM's network, pharmacies are credentialed using the PBM's criteria. Activities may include review of pharmacy licenses, staff training, policies and procedures, and/or observation visits.

ii. Monitoring: Claims submitted from pharmacies are statistically analyzed through the PBM's internal algorithms to identify potentially aberrant claims for further review.

iii. Auditing: Audit activities include prospective and retrospective statistical review of claims for potentially aberrant claims and communication to the pharmacy for correction (pre-payment) and/or requests for documentation to validate the claim(s).

4. Other broad methods of surveillance are implemented through a number of processes, such as periodic claims audits and utilization management controls. Each DHMP department is encouraged to provide input into improving methods to detect fraudulent behavior.

H. **Special Investigations Unit Committee (SIC)**

1. The SIC oversees FWA activities, including the execution of the annual FWA work plan (which contains planned case work and ad hoc referrals) and the performance of FWA audits and investigations by DHMP's contracted vendors.

2. The SIC is a sub-committee of DHMP's Compliance Committee and reports of medium to high risk activity and investigations are reported at least quarterly to the Compliance Committee.

3. High risk FWA activity is reported to the DHMP Finance, Audit and Compliance Committee of the Board of Directors and the DHMP Board of Directors as necessary.

I. **Incident Review and Investigation**
An investigation of a particular practice or suspected violation shall involve a review of the relevant documentation and records, interviews with staff, and analysis of applicable laws and regulations. The results of any investigations shall be thoroughly documented. Investigation records shall include a description of the investigative process, copies of interview notes and key documents, a log of individuals interviewed and documents that are reviewed, the results of the investigation, and any disciplinary or corrective actions taken. Precautions shall be taken to ensure that critical documents are not destroyed and are retained in accordance with statutory guidelines regarding retention. A detailed record is maintained to track all reported incidents to ensure an audit trail for each case.

EXTERNAL REFERENCES

A. 42 C.F..R 422.503 – General Provisions

B. 42 C.F.R. 423.504 – General Provisions

C. 42 C.F.R. § 438.608 Subpart H— Additional Program Integrity Safeguards

D. CMS Prescription Drug Benefit Manual Chapter 9 - Compliance Program Guidelines and Medicare Managed Care Manual Chapter 21 – Compliance Program Guidelines

E. C.R.S. §10-1-128 – Fraudulent Insurance Acts

F. Child Health Plan Plus (CHP+) contract between the Colorado Department of Health Care Policy &

Financing and Denver Health Medical Plan (DHMP), Inc. (hereinafter referred to as the CHP+ contract).

G. Colorado Division of Insurance Regulation 6-5-1 - Concerning the Reporting of Suspected Insurance Fraud

H. Medicaid Choice contract between the Colorado Department of Health Care Policy and Financing and Denver Health Medical Plan (Medicaid Choice)

DHMP RELATED DOCUMENTS

A. Provider/Vendor/Subcontractor Overpayments Policy

B. Record Retention and Destruction

C. Special Investigations Sub-Committee Charter

DHHA RELATED DOCUMENTS

A. Denver Health Code of Conduct

B. Denver Health Enterprise Compliance Program

C. Non-Retaliation, HR Principle and Practice

D. False Claims, Fraud, Waste and Abuse Policy, HR Principle and Practice

E. Records Retention

Approval Signatures

Step Description	Approver	Date
Final Signatory	Greg McCarthy: Executive Director, Managed Care	06/2021
Compliance Committee	Lisa Artale Bross: Compliance Manager	06/2021
Chief Compliance and Audit Officer	Catharine Fortney: Chief Compliance And Audit Officer	06/2021
Legal	Jordan Clothier: Senior Staff Attorney	06/2021
SIU Committee Chair	Bridget Johnson: Director of Compliance and Internal Audit	05/2021
Program Integrity	Josh Holte: Director of Claims	05/2021
Formatting	Stacy Grein: Compliance Specialist	05/2021

	Lisa Artale Bross: Compliance Manager	05/2021

Older Version Approval Signatures

Legal	Jordan Clothier: Senior Staff Attorney	04/2020
Legal	Jordan Clothier: Senior Staff Attorney	04/2020
Compliance Committee	Gina Eisenach: Dir Compliance & Int Audit	04/2020
Formatting	Aryn Thedens: Compliance Auditor	04/2020
SIU Committee Chair	Bridget Johnson: Internal Audit Manager	04/2020
	Lisa Artale Bross: Compliance Manager	04/2020