SPECIAL INVESTIGATION PROGRAM MANUAL

ANTI-FRAUD PLAN
FOR
DENVER HEALTH MEDICAL PLAN

Denver Health Medical Plan's Anti-Fraud Program includes the following:

(a) A description of procedures for detecting and investigating possible fraudulent insurance acts;
(b) A description of procedures for the mandatory reporting of possible fraudulent insurance acts to the Centers for Medicare and Medicaid Services;
(c) A description of the plan for antifraud education and training of the company's claims adjusters or other personnel; and
(d) A written description or chart outlining the organizational arrangement of the antifraud personnel who are responsible for the investigation and reporting of possible fraudulent insurance acts.

Denver Health Medical Plan ("DHMP"), is a Colorado Health Maintenance Organization, submits that DHMP is in compliance with 42 C. F. R.§ 423.504(b)(4)(vi)(H), in that they have a Special Investigation Department (SIU) service, and has completed and maintains the following Antifraud Plan ("Plan").

The components of the Anti-Fraud Plan are as follows:

I. Prospective Fraud Process
II. Retrospective Fraud Recovery Process
III. Reporting Insurance Fraud
IV. Education and Training
V. Primary Contact Persons/Organizational Chart

PROSPECTIVE FRAUD PROCESS

Introduction

DHMP Health Plans, Inc. ("DHMP") is a health maintenance organization (HMO), duly licensed in the State of Colorado. DHMP provides comprehensive and high-quality health coverage, through its various insurance products to its member beneficiaries in Colorado.

Internal Fraud Prevention, Detection, and Investigation

DHMP has adopted certain fraud prevention, detection, and investigation procedures. Following is a summary of processes that serve to prevent internal fraud at DHMP.

Comprehensive Internal Compliance Program

The current Compliance Program provides, among other things, for the reporting of compliance issues. Employees may report improper activity to their supervisors, the Chief Compliance Officer, or anonymously. The Compliance Program expressly prohibits retaliation against those who, in good faith, report concerns or participate in the investigation of compliance concerns. The Compliance Program provides that compliance concerns will be investigated rigorously and resolved promptly by the Chief Compliance Officer, Finance Department, SIU, Human Resources, or other departments as appropriate, depending upon the nature of the violation.

External Fraud Prevention and Detection

DHMP strives to prevent, deter, and detect fraud and/or abuse perpetrated by providers and members against DHMP, by receiving referrals from a variety of sources, and through the use of sophisticated fraud detection technology.

Any employee can report suspected incidents of fraud and is encouraged to do so. It is strongly encouraged that suspected fraud be reported to the employee's supervisor who may then convey it to the SIU. Supervisors should routinely assure that all fraud allegations are reported.

"Tips" are accepted directly from any employee, anonymously if preferred. This will insure that personnel are not discouraged from submitting referrals. Referrals are reviewed by the SIU, to determine the appropriate course of action. Any suspicion of an inappropriate or fraudulent act must be reported.

Fraud Detection Technology

The SIU will use several advanced technological tools in preventing and detecting fraud. Data will be routinely analyzed by the SIU. This data analysis will be critical in the identification of fraud patterns and abusive providers. Reports will be generated to identify potential fraud schemes and abusive providers. Once a fraud scheme or abusive provider has been identified an investigation will be initiated.

Provider Integrity Database

The "Tips" portion of this database is populated by tips from reliable sources (i.e., Members, State DOI, FBI, etc.). Once a provider has been investigated, the information will remain active if allegations were proven and/or savings realized. If allegations were unproven, then provider information will be maintained, in an inactive status.

Disclaimer

Note: Being identified through or referenced in the database does not necessarily represent wrongful past or current practices; only that enough information is available to warrant prior-to-payment review of current and future claims. Inclusion in the Provider Integrity Database should not be construed as a basis for automatically denying providers' access to networks, claims denial, etc.

SIU Case Database

The SIU Case Database is a case-tracking database designed and used by the SIU to manage investigation-related information. Providers, members, and schemes previously investigated and included in the SIU Case Database serve as sources for use in detecting fraud and/or abuse.

Fraud/Suspicious Claim Referral Sources

Although a report of suspicious activity may not always result in a conclusion of fraud, a formal review by the SIU may be warranted due to unique health plan specific guidelines. Such activity may be initially detected and reported in a variety of ways, namely internally, externally, and through system referrals.

Internal referrals include discrepancies noted by personnel such as Claims Processors, Actuary, Internal Auditors, and Customer Service Representatives. Any employee who becomes suspicious of any claim form, other document, or activity, is encouraged to report the matter to the SIU.

The identification and prevention of fraud is a cooperative effort, involving all employees. All employees are required to cooperate in any investigation conducted by DHMP.

Through the course of its investigations, the SIU may work with any other departments within DHMP to review questionable claims and provide guidance.

Ongoing computer-based analysis of provider or member behavior data is important. Patterns of over utilization, exorbitant billing, or other unusual billing practices must be addressed. Additionally, proprietary system flags or edits within the claims systems automatically segregate claims with certain predetermined characteristics.

Referrals

Referrals can originate from claims personnel, medical management, medical claim review staff, provider relations representatives, medical directors, quality assurance staff, utilization review personnel and provider credentialing; other medical providers; through involvement in the National Health Care Antifraud Association; from law enforcement agencies such as The Department of Health and Human Services, the Colorado Department of Insurance, the FBI, or other such agencies.

Investigative Process

The Manager of the SIU determines investigation priorities and assigns cases to the SIU staff.

The SIU is responsible for the following:

- Establishing a case file for each referral as warranted
- Obtaining necessary DHMP documentation and supporting documents for all case files, including copies of claims, contracts, correspondence, and other relevant documentation
- Conducting a case investigation to conclusion in accordance with the procedures established by the SIU

The SIU conducts inquiries, audits, investigations, and other related activities, which may involve:

- Data collection
- Conducting interviews
- Performing data analysis
- Coordination with the Division of Insurance and other federal and state agencies, as necessary

Initial Handling of Referral

Upon receipt of the referral, various investigative reports are processed regarding the provider, member, or scenario and those reports are provided to the SIU staff for initial evaluation. This process involves:

- Determining if the referral merits being investigated
- Review all submitted documents for suspicious claim indicators.
- Identify additional information needed to properly evaluate the referral
- Determine whether additional investigation of the referral is warranted depending upon findings after initial evaluation.
- If during the initial evaluation the possibility of fraud is eliminated, the referral is then returned to originator and no action will be taken
- If fraud cannot be definitively eliminated, the referral becomes an investigation, and a case is established.
- An SIU staff member enters the case into the SIU Case Database. This task incorporates the referral into SIU tracking system and creates a case file for the investigation.
- After the case is logged into the SIU Case Database, an SIU staff member confirms the accuracy of all information entered.

The case must be fully investigated, for which the staff member formulates an investigative plan.

Planning the Investigation

The SIU staff member must gather information from various sources in planning the course and strategy of the investigation. Information is gathered from the following sources:

Claims Database. The "Claims" section of the Claims Database includes a listing of providers linked by tax identification numbers (TIN).

Closed Cases. Recently closed cases are reviewed to identify patterns and/or schemes. Closed cases can be accessed through the SIU Case Database or hard-copy files.

Other SIU Staff Consulting with a staff member, who has previous experience with a particular provider, is useful in obtaining insight into that provider's methods, billing practices, etc.

Medical Records and Supporting Documentation. Medical records are examined to determine if the services being claimed were delivered, and how the services compare to what is included in the claim.

Based upon the staff member's review of investigative sources, the staff member will establish an investigative plan.

Conducting the Investigation

Pursuant to the investigative plan, one or all of the following resources may be utilized to assure a complete and thorough investigation:

Patient/Member Information. Interviewing patients, via telephone contact, enables the staff to confirm or refute whether the services charged were actually rendered.

Provider/Billing Entity Information. Verifying providers' licenses, and searching for the existence of disciplinary action, is useful in determining whether claims were submitted for services performed by qualified medical professionals.

Contacting providers' offices to confirm telephone numbers and addresses assist in ascertaining the legitimacy of the provider and/or claim. Searching for mail-drop listings may also reveal the existence of fabricated provider identities or billing entities.

Clinical Review. Cases may involve charges for services that do not reflect what service was actually rendered. A medical record review may be required to determine if the service rendered was the actual service that was billed.

Gathering and Collecting Evidence. Original documentary evidence is collected, marked, and maintained by staff. Interviews may be obtained from parties who can identify characteristics of exhibits, including authenticity of signatures of handwriting, of acknowledgement that the signature or content contained in the document is his/her own, prepared by that party, or that another party was observed preparing or signing such document.

After evidence is gathered, the staff member carefully records information regarding the evidence in files and/or on the case tracking system.

The SIU staff shall be responsible for ensuring that all evidence on cases referred for investigation including, but not limited to, checks issued in payment of claims, statements, original receipts, and original documents submitted by a person of entity in support of or in opposition to a claim, are identified, collected, and preserved in order to be submitted to the appropriate regulatory and/or law enforcement agencies.

Interviews. SIU staff frequently interview external sources. Interview responses often trigger additional evidence collection opportunities. Questions are prepared according to the facts. Interviews are conducted to establish the factual elements of a case (i.e., Who, What, When, Where, Why, and How).

Documentation/Report Writing. SIU staff members' documentation should include the following items:

- Case Summary;
- Member Interview;
- License Verification;
- Clinical Review;
- Other Sources of Information (i.e., interviews, documents examination of benefits, etc.);

- Statements, and Documentary Exhibits.

Concluding the Investigation. After the investigation has been completed, the staff member prepares a Comprehensive Investigation Report and forwards the report to the Manager of the SIU. The report summarizes the case and the results of the investigation, including the Investigator's findings.

Initiate A Resolution And/Or Prevention Strategy. After a case is investigated and documented, the final stage of the investigation is to determine the appropriate resolution. The Manager of the SIU makes case resolution decisions. The options considered for resolution include, but are not limited to:

Closing The Case. Closing the case may be the best option when the evidence does not support inappropriate behavior, or the legal or medical merits of the case are ill defined.
Implement Prospective Controls. When the results of an investigation do not clearly indicate that all of the elements of fraud have been established, the provider may be identified in the system to monitor future activity to determine if a pattern of suspicious billing practices persists.

Litigation. It may be appropriate for DHMP's Legal Counsel to file a civil suit against a provider or member to recover defrauded funds. DHMP's Legal Counsel, or their attorneys, determine the legal merits of each case and proceed accordingly.

Referring Suspected Fraud to Authorities. The Manager of the SIU will make the decision if a case warrant being reported to either state or federal agencies. When a case rises to the level of reportable fraud, according to federal and state statutes, the Manager of the SIU will submit case reports upon notification and approval by senior management, to the appropriate regulatory agency.

RETROSPECTIVE FRAUD PROCESS

The Retrospective Fraud Process is similar to prospective fraud process but is conducted after services have been rendered and the claim for services has been paid. Although the SIU's goal is to identify fraud before claims are paid, there are certain instances were only a retrospective process works. The recovery process consists of the following steps:

Detection
- Referrals are collected from various sources including data mining, internal or external tips, government sources, professional organizations, etc.
- The quality and credibility of allegations or suspicious situations are assessed. Initial exposures and recovery potential are identified to determine if a case should be opened.

Investigation

- Cases are prioritized pursuant to commonly accepted business practices and business objectives.
- An investigative action plan/timeline is developed to guide the investigation. The action plan is periodically reviewed and revised as circumstances change.
- Relevant claim data for the period in question is obtained and reviewed.
- Evidence is gathered to support data analysis and allegations.
- An investigative summary/report is prepared which summarizes the investigative findings and displays a comprehensive understanding of the facts and financial implications.

Resolution

Investigative findings are communicated to appropriate business partners. An appropriate resolution strategy is selected. Following are the strategies most commonly pursued in resolving recovery cases:

- **Approaching the provider for repayment.** Attempting to collect overpayments directly from the provider may expedite the recovery process and cost less than filing a civil suit to collect the funds
- **Educating the provider.** If investigation results indicate that the claim contained unintentional billing errors, it is necessary to contact the provider and advise of the errors and provide tips on appropriate billing techniques. (Note: This step is coordinated with DHMP's ongoing claims recovery process.)
- **Implementing Prospective Controls.** When the result of an investigation does not indicate a clear case of fraud, the SIU may flag a provider or member in the system to monitor future activity to determine if a pattern of fraud or abuse is evident.
- **Closing the investigation.** This may be the best option when the evidence does not support inappropriate payments or the legal of medical merits of the case are ill-defined
- **Referring suspected fraud to authorities.** Reporting the provider to CMS, State Medical Board, or other regulatory agencies, or pursue network dismissal.
- **Mediate or arbitrate the matter.** Attempting to mediate or arbitrate the matter, which generally costs less than filing a civil suit and is a quicker means of settling a matter.
- **Litigating.** It may be appropriate to file a civil suit against a provider or member to recover defrauded funds. DHMP's legal counsel will determine the merits of each case and proceed as they determine is legally sound.
- **Recovery and action.** Pursuing recovery and determine corrective action to prevent future losses.

REPORTING INSURANCE FRAUD

A fraudulent insurance act is committed if a person knowingly and with intent to defraud presents, causes to be presented, or prepares with knowledge or belief that it will be presented, to or by an insurer/HMO, self-insurer, agent, broker, etc., any written statement as part of, or in support of, an application for insurance, rates, claims, or any other benefit, which the person knows to contain materially false information concerning any material fact. Also, a fraudulent insurance act is committed if the person conceals, for the purpose of misleading another, information concerning any material fact.

DHMP and/or the SIU shall cooperate fully with the Centers for Medicare and Medicaid Services (CMS) and/or other law enforcement agencies in their prosecution or additional investigation of cases reported on behalf of DHMP.

EDUCATION AND TRAINING

DHMP Employee Education/Fraud Awareness Training

Anti-fraud education and training of claims adjusters or other appropriate personnel is highly recommended.

- The corporate training is broad in scope. The intent is to address health insurance fraud and the impact that it can have on DHMP. The program is designed to be web base. Its objectives of web base training are to provide employees with specific tools to detect fraud, instruct them in the procedures for reporting cases of suspected fraud, and create an awareness of the staggering financial and service consequences of fraud.

- The focus will be on the critical role that each employee plays in eradicating fraud and abuse committed against DHMP and its members. Highlights of the program include:

- Definition of Fraud and Abuse;
- Tools for fraud detection ("red flags");
- The SIU's prevention efforts;
- Reporting fraud and abuse;
- Review of actual investigations;
- Current industry trends in the fraud and abuse arena.

Claims/Customer Service personnel should attend Fraud Awareness Training every two years. This attendance will be tracked by the SIU. Regular fraud awareness bulletins will be distributed to all employees on a periodic basis.

Investigator Education/Training

Upon hire, SIU staff members will complete a comprehensive fraud detection-training course that will provide the new staff member with information about the SIU and the Anti-Fraud Program as well as material regarding techniques used to combat fraud and abuse. In the overviews given by each of the instructors, tips and case examples are shared by the prospective instructor and investigative teams as well as the process for case development. All new hires within the SIU will receive the same training whether they are assigned to investigative functions or other duties (i.e. detection technology, etc).

With respect to on-going training, The Manager of the SIU will ensure that SIU staff members attend periodic training sessions throughout the year. Staff members will receive technical fraud training through attendance at the National Health Care Anti-Fraud Association's various seminars and workshops. Staff members who attend participate in the sessions that relate most directly to their specialty or position.

Additional training sessions will include technical/computer training that will occur throughout the year and address various computer applications used by the investigator. Periodically, internal training sessions are presented by various speakers/units from various vendors, and consultants from outside the organization related to SIU staff skill enhancement and they will address specific investigative skills to increase the staff's knowledge of various products and services offered to detect and deter potential fraud scenarios.

SIU staff will be provided with and follow SIU Investigation Manual in conducting investigations. The SIU's Operations Manual will include, but will be not limited to, the following topics:

- Information for SIU staff regarding general investigation guidelines; conducting interviews; report writing; information disclosure; law enforcement relations;
- The process to be employed when a suspicious claim is identified;
- The suspicious claim indicators;
- The duties and functions of the SIU.

PRIMARY CONTACT PERSONS/ORGANIZATIONAL CHART

Any inquiries regarding DHMP's Anti-Fraud Plan should be directed to:

Payment Integrity Department
Attn: SIU Manager
938 Bannock St
Denver. Colorado 80204
Tele: TBD