A Guide to the Compliance Program

To report **suspected fraud and abuse** or other **violations of company policy**, call **1-877-879-9137** or go to **www.hfcompliance.ethicspoint.com**

A Guide to the Compliance Program

To report **suspected fraud and abuse** or other **violations of company policy**, call **1-877-879-9137** or go to **www.hfcompliance.ethicspoint.com**

NOTE: For further details on the contents of this guide, the complete Compliance Manual is available upon request by contacting the Compliance Officer at 1-212-453-4495. It is also available on the Healthfirst Intranet.

Healthfirst's Commitment

Healthfirst is committed to the successful implementation of its Compliance Program.

The goal of the Compliance Program is twofold: 1) to reduce or eliminate fraud, abuse, and inefficiencies and 2) to ensure the company adheres to all applicable Federal and State regulations, as well as to all sub-regulatory guidance, which includes manuals, training materials, and guides produced by governmental agencies that oversee the various government-sponsored programs.

This is accomplished by applying processes developed to reduce the probability of unlawful and improper conduct and reinforce Healthfirst's commitment to "zero tolerance" for such activities. Furthermore, each employee is responsible for understanding and complying with Federal and State regulations. Any employee who is knowingly not in compliance with the regulations or who is aware of such noncompliance and fails to report it will be subject to disciplinary action, up to and including termination.

If you have questions, concerns, or comments on improving the Program, contact the Compliance Officer at 1-212-453-4495.

Table of

Contents

Overview—Compliance Program 3

Compliance Policy 3

Compliance Code of Conduct 4

Fraud Prevention and Detection 5

Identifying Inappropriate Activities 6

Reporting Inappropriate Activities 9

Relevant Laws and Regulations 10

Health Insurance Portability and Accountability Act (HIPAA) 12

STRATEGY
COMPLIANCE
STANDARDS
CONTROL
RISK
RULES
POLICY
LAWS
GOVERNANCE
SECURITY

Overview–Compliance Program

Healthfirst is committed to ensuring compliance with all Federal and State regulations, as well as with organization policies and procedures. Healthfirst maintains a proactive approach to regulatory compliance, which is demonstrated by its ongoing Compliance Program.

The implementation of an effective Compliance Program provides many benefits to Healthfirst, as well as to its employees. Healthfirst's Compliance Program:

- Demonstrates to employees and contracted entities its commitment to responsible corporate conduct.
- Establishes internal controls to assure compliance with federal and state regulations and internal guidelines.
- Creates and reinforces an environment that encourages employees to report potential problems.
- Centralizes the responsibility for interpreting and distributing compliance information and for preventing unlawful and unethical conduct.
- Ensures prompt and thorough investigation of possible misconduct by corporate officers, management, employees, and contracted entities.

Compliance Policy

Healthfirst maintains a strict policy of zero tolerance toward fraud and abuse. The purpose of investigating these activities is to protect the member, government, and/or Healthfirst from paying more for a service than it is obligated to pay.

However, Healthfirst's zero tolerance policy is not limited to fraud and abuse cases; it also includes willfully failing to comply with regulations, harassment, and any other inappropriate activities. All employees have an obligation to report all alleged wrongdoings. Those who knowingly fail to comply with the regulations, or those who are aware of such noncompliance and fail to report it, will be subject to disciplinary action, up to and including termination.

Individuals who engage in any inappropriate activity—alone or in collaboration with another employee, a member, or a provider—are subject to immediate disciplinary action, up to and including termination.

For further information regarding our commitment to detecting, investigating, and preventing fraud and abuse, please see the Fraud Prevention and Detection section.

Compliance Code of Conduct

The Healthfirst Code of Conduct highlights the principles, policies, and procedures that underlie Healthfirst's fundamental principles and embody our culture as a company. All Healthfirst employees must review the Code and understand how it applies to their work. In order to provide the best value for Healthfirst members and providers, Healthfirst employees must be in full compliance with Federal, State, and local laws and regulations. The Code of Conduct summarizes these important standards and also provides guidance to assist with the responsibility to behave ethically, legally, and responsibly in the marketplace. The Code is organized into three sections—Our Workplace, Our Relationships, and Our Business—to guide principled decision making and to address ethical situations that may arise within each of these settings.

The Code also emphasizes Healthfirst's commitment to the highest standards of ethical business dealings and our zero-tolerance policy for fraud and abuse or other inappropriate activities. The Code of Conduct, in conjunction with the guidance outlined in the sections below, provides instructions on how to identify, detect, and prevent fraud and abuse, as well as references several channels through which it can be reported.

The Code of Conduct applies to all Healthfirst employees, officers, and directors. It also applies to consultants, agents, and contractors, as well as to those who work on our behalf or perform work on Healthfirst's premises.

The Code of Conduct can be found on the Healthfirst Intranet, under the Compliance Department, Compliance Resources.

Fraud Prevention and Detection

As previously stated, Healthfirst maintains a strict policy of zero tolerance toward fraud and abuse. The purpose of investigating these activities is to protect the member, government, and/or Healthfirst from paying more for a service than it is obligated to pay. Therefore, Healthfirst established a Special Investigations Unit (SIU), which ensures that Healthfirst is in compliance with State and Federal regulations as they relate to this area.

The SIU is chiefly responsible for accepting referrals both from outside the company and from within the company for investigation to determine if fraud has possibly occurred. Therefore, Healthfirst employees and contracted entities have a responsibility to report any inappropriate activities to the SIU, the Regulatory Affairs department, or their immediate supervisor, if applicable.

This guide outlines the process for reporting such activities in the "Reporting Inappropriate Activities" section.

In order to report inappropriate activities, it is important to be able to identify such behavior.

What is Fraud?

Fraud is intentional deception or misrepresentation whereby the person or entity knows that the deception could result in some unauthorized benefit to himself/herself or some other person.

Basic examples of healthcare fraud are a provider billing for services not actually rendered or an individual using a member's identification card to obtain healthcare benefits.

What is Abuse?

Abuse is an action inconsistent with accepted, sound business or fiscal practices that directly or indirectly results in unnecessary costs to the organization or to the Medicaid, Medicare, or other client program.

Basic examples of abuse of the healthcare payment system are providers performing and billing for services not medically necessary, and upcoding of rendered services in order to increase reimbursement (such as billing a "Brief" office visit as a "Moderate Complexity" office visit).

The real difference between fraud and abuse is the person's intent.

In the end, both activities detract valuable resources from the organization that would otherwise be used to provide more services to our members.

healthfirst

Identifying Inappropriate Activities

Common Methods of Fraud and Abuse Used by Healthcare Providers

Fabrication of Claims: In the outright fabrication of claims or portions of claims, fraud perpetrator uses legitimate patient names and insurance information either to concoct entirely fictitious claims or to add to otherwise legitimate claims fictitious charges for treatments or services that were never provided or performed. Examples are as follows:

- Submitting claims for services not rendered.
- A provider who, using existing information on his or her patients, creates claims for office visits or services that never took place.
- A provider who, in the course of billing for actual patient treatments, adds charges for X-rays or laboratory tests that were never performed.
- A Durable Medical Equipment provider submitting claims for equipment and supplies that were never delivered, or continuing to submit claims for rented equipment after it has been picked up.

Falsification of Claims: In the falsification of claims, the perpetrator makes a material and intentional misrepresentation of one or more elements of information in the claim for the purpose of obtaining a payment to which he or she is not entitled. Examples are as follows:

- A provider performs medically unnecessary services solely in order to bill and be paid for doing so.
- A provider falsifies symptoms or other diagnostic information in order to obtain payment for an uncovered service. This is somewhat more common in certain specialties, such as cosmetic surgery.
- A provider falsifies the dates on which services were provided so that they fall within a given eligibility period of the member.
- A provider falsifies the identity of the provider of services so as to obtain payment for services rendered by a non-covered and/or non-licensed provider. (For example, submitting claims for clinical social worker services as psychiatric treatment provided by a licensed psychiatrist, or billing fitness center massages as a licensed physical therapy.)
- A provider upcodes the services rendered to obtain greater reimbursement.
- Upcoding of Evaluation and Management services to indicate a greater complexity of medical decision making than was actually rendered; encounters that required straightforward decision making are reported as having required highly complex decision making.
- Reporting more intensive surgical procedures than were actually performed.
- Anesthesiologist bill for more intensive surgical procedures than reported by the surgeon.

Unbundling: Provider submits a claim reporting comprehensive procedure code (Resection of small intestine) along with multiple incidental procedure codes (Exploration of abdominal and Exploration of the abdomen) that are an inherent part of performing the comprehensive procedure.

Some providers may submit the unbundled procedures on multiple claims in an attempt to bypass bundling edits in the claims-processing system.

Fragmentation: Provider submits a claim with all the incidental codes or itemizes the components of the procedures/services (Antipartum care, Vaginal delivery and Obstetric care) which includes the three components. Some providers may submit the unbundled procedures on multiple claims in an attempt to bypass fragmentation edits in the claims-processing system.

Duplicate Claim Submissions: Submitting claims under two Tax Identification Numbers to bypass duplicate claim edits in the claims-processing system.

Common Methods of Fraud and Abuse Used by Members

- Sharing of an Identification Card, allowing a non-eligible person to try to obtain medical services.
- Submitting claims for services that were not rendered.
- Participating in diagnosis gaming by a provider—such as a plastic surgeon—to obtain reimbursement for services usually not covered.
- Reporting non-family members as dependents in order to obtain medical services.
- Failing to report information concerning other coverage.
- Claims submitted for services rendered in third world countries.
- High dollar out-of-the-service-area claims where it is doubtful that the member would have had the cash available while traveling to pay the provider.
- Lack of/or questionable receipt.

Common Methods of Fraud and Abuse Used by Employees or Health Plans

Enrollment of an individual or entire family not eligible for coverage.

- Failure to remove individuals or families when they no longer qualify for healthcare coverage.
- Discriminating against applicants for Healthfirst programs based on their health status, also known as “cherry-picking.”
- Submitting inaccurate claims or encounter data to the State or CMS.
- Improper enrollment of a person into a Healthfirst program without their consent.
- Knowingly submitting inaccurate expense reports.
- Knowingly submitting claims to the Medicaid program for a member or members not actually served by Healthfirst.
- Stealing or inappropriately using corporate resources.

healthfirst

Common Methods of Fraud and Abuse Used by Others

Fictitious Providers: There has been fraud where perpetrators obtain current membership information from operatives working in the billing offices of legitimate providers (usually hospitals) and submit claims, usually on the HCFA 1500 claim form.

Indicators of Fraud

There are many indicators of fraud, which, if noticed by Healthfirst staff members, should be brought to the attention of the Special Investigations Unit. A list of the most common indicators follows:

- Addition of services to bill
- Claims for more than one pharmacy for the same member in a short period of time
- Claims for non-emergency services on weekends and holidays
- Claims that have been handwritten or that contain changes made by hand
- Diagnosis inconsistent with age or sex
- Eligibility file date of birth does not match date of birth on claim (indication that an identification card has been shared)
- Impossible or unlikely services for age or sex
- Inconsistency between provider type and/or specialty and services rendered
- Inconsistency between services billed and medical history
- Indication that coinsurance has been waived (illegal)
- Inordinate incidence of diagnoses of rare diseases
- Inquiry from provider regarding receipt of any unexpected payment
- Large distance between providers and member location
- Mail to members and providers returned as undeliverable, etc.
- Not on standard claim forms such as UB92 or HCFA 1500
- Provider advertisement for free services, drugs, supplies, or durable medical equipment
- Provider and members demanding immediate payment
- Providers and members reporting the receipt of unexpected payments
- Providers and members warning of legal action or reporting to regulatory authorities if claims not paid immediately
- Providers demanding immediate payment for claims
- Providers demanding immediate replacement of lost or stolen checks
- Providers insisting on using private mail services for claims submission and payment
- Providers with more than a few lost or stolen checks
- Reluctance or failure to submit medical records when requested
- Submission of identical claims for more than one member or family member
- Unprofessional medical terminology (cold, stomachache)
- Unusual time between service and claim submission
- Vague diagnoses accompanied by extensive services

Reporting Inappropriate Activities

Healthfirst has developed a variety of methods for employees, enrollees, and other parties to report a potential violation of the organization's compliance polices or of federal and state regulations.

The Special Investigations Unit (SIU) shall facilitate obtaining information on Potential fraud, abuse, and inappropriate activities. The methods listed below ensure confidentiality and do not result in retaliation against the individual(s) reporting such allegations.

You can report suspected cases of fraud and abuse or other violations of company policy in whatever manner you feel most comfortable:

- Call the toll-free Confidential Compliance Hotline at 1-877-879-9137;
- Report via the Confidential Website, www.hfcompliance.ethicspoint.com;
- Report it directly to your Supervisor, the Compliance Officer, Human Resources, or the Legal department by phone, email, or in person.

All of the above communications are confidential to the extent possible. Additionally, the above are logged and, if appropriate, investigated and summarized to the Audit and Compliance Committee. If you have reported an issue and you believe that Healthfirst did not fully investigate or act upon your referral, you may also bring your issue to the attention of the government. The False Claims Act section provides an overview of how everyday citizens can bring suit or an action to the government's attention.

Confidential Compliance Hotline
1-877-879-9137

Confidential Website
www.hfcompliance.ethicspoint.com

Supervisor, Compliance Officer,
Human Resources,
Legal Department
phone, email, or in person

healthfirst

Relevant Laws and Regulations

Deficit Reduction Act

As a participant in the Medicaid Program, we must comply with the terms of the Deficit Reduction Act of 2005 (the "DRA"). The DRA, specifically Section 6033, entitled "Employee Education About False Claim Recovery," which was effective January 1, 2007, requires any organization that receives $5 million or more in Federal Medicaid funds annually (including payments from managed care companies such as Healthfirst) to adopt a compliance program in accordance with federal law and to inform its employees and any contractor or agent of the terms of the False Claims Act. Any organization that does not comply with the requirements may be denied Medicaid reimbursement. You should carefully consult with your attorney to determine if you are subject to this requirement.

False Claims Act

31 U.S.C. 3729 – 3733P.L. 2007, Chapter 265, (as amended by P.L. 2009, Chapter 265)

The federal government amended the False Claims Act (FCA) to make it a more effective tool. Using the False Claims Act, private citizens (i.e., whistleblowers) can help reduce fraud against the government. The act allows everyday people to bring suits against groups or other individuals that are defrauding the government through programs, agencies, or contracts (the act does not cover tax fraud).

For the purposes of this policy, "knowing and/or knowingly" means that a person, with respect to the information, has actual knowledge of the information; acts in deliberate ignorance of the truth or falsity of the information; or acts in reckless disregard of the truth or falsity of the information. No proof of specific intent to defraud is required.

Both State and Federal False Claims Acts (FCAs) apply when a company or person:

- Knowingly presents (or causes to be presented) to the federal government a false or fraudulent claim for payment
- Knowingly uses (or causes to be used) a false record or statement to get a claim paid by the federal government
- Conspires with others to get a false or fraudulent claim paid by the federal government
- Knowingly uses (or causes to be used) a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the federal government

Examples of the type of conduct that may violate the FCA include the following:

Knowingly submitting premium claims to the Medicaid program for members not actually served by Healthfirst

- Knowingly failing to provide members with access to services for which Healthfirst has received premium payments
- Knowingly submitting inaccurate, misleading, or incomplete Medicaid cost reports

False Claims Act Penalties

Those who defraud the government can end up paying triple (or more than) the damage done to the government or a fine (between $10,781 and $21,563) for every false claim, in addition to the claimant's costs and attorneys' fees. These monetary fines are in addition to potential incarceration, revocation of licensures, and/or becoming an "excluded" individual, which prevents an individual from being employed

in any job that receives monies from the federal government, the state government, or both.

FCA: Whistleblower Protections

The False Claims Act allows everyday people to bring suits against organizations or individuals who are defrauding the government (but the act does not cover tax fraud). These individuals are commonly known as "whistleblowers." If the government moves forward with a case, the individual who brings the suit is generally entitled to receive a percentage of any recovered funds once a decision has been made. If the government decides not to pursue the case, then the individual must pursue the issue on his or her own and, if successful, then he or she would be entitled to a percentage of any recovered funds as well.

Federal statutes and related state and federal laws shield employees from retaliation for reporting illegal acts of employers. An employer cannot retaliate in any way, such as discharging, demoting, suspending, or harassing the whistleblower. If an employer does retaliate, the employee may be entitled to file a charge with a government agency, sue the employer, or both.

To report information about fraud, waste, or abuse involving Medicare or any other healthcare program involving only federal funds, call the toll-free hotline established by the federal Office of Inspector General in the U.S. Department of Health and Human Services. The hotline number is 1-800-HHS-TIPS (1-800-447-8477).

For more information about this hotline and about other ways to contact the Office of Inspector General, you can go to https://oig.hhs.gov/fraud/report-fraud/index.asp.

Stark Law

The Stark Law, with several separate provisions, governs physician self-referral for Medicare and Medicaid patients. Physician self-referral is the practice of a physician referring a patient to a medical facility in which he has a financial interest, be it ownership, investment, or a structured compensation arrangement.

The Omnibus Budget Reconciliation Act of 1989 also bars self-referrals for clinical laboratory services under the Medicare program. The law included a series of exceptions to the ban in order to accommodate legitimate business arrangements. The Omnibus Budget Reconciliation Act of 1993 expanded the restriction to a range of additional health services and applied it to both Medicare and Medicaid. The Social Security Act prohibits physicians from referring Medicare patients for certain designated health services to an entity with which the physician, or a member of the physician's immediate family, has a financial relationship—unless an exception applies. It also prohibits an entity from presenting, or causing to be presented, a bill or claim to anyone for a health service furnished as a result of a prohibited referral.

Violations of the Stark Law and the practice of physician self-referral are to be reported to the Centers for Medicare and Medicaid Services via their self-disclosure process.

Anti-Kickback Statute

The Medicare and Medicaid Patient Protection Act of 1987 provides the basis for this statute. It provides for criminal penalties for certain acts which impact Medicare and Medicaid or any other federally funded or state-funded program. If you solicit or receive any remuneration in return for referring an individual to a person (doctor, hospital, and provider) for a service for which payment may be made, it can be seen as a potential kickback. Remuneration includes payment, monies, or any goods or services from any healthcare facilities, programs, or providers.

Federal Program Fraud Civil Remedies Act

31 U.S.C. 3801-3812

For a copy of this citation, please visit: https://www.federalregister.gov/articles/2009/06/04/E9-12170/program-fraud-civil-remedies-act

This act provides federal administrative remedies for false claims and statements, including those made to federally funded healthcare programs. Current civil penalties are $10,781 for each false claim or statement and an assessment in lieu of damages sustained by the federal government of up to double damages for each false claim for which the government makes a payment. The amount of the false claims penalty is to be adjusted periodically for inflation in accordance with a federal formula.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy

The HIPAA Privacy Rule requires providers to take reasonable steps to protect and safeguard the Protected Health Information ("PHI") of members/patients. A member's PHI is subject to the protections established by the Privacy Rule and under the contractual relationship between Healthfirst and the member, and between Healthfirst and the provider or FDR. PHI includes information regarding enrollment with Healthfirst, medical records, claims submitted for payment, etc. Such PHI must be safeguarded and held in strict confidence, so as to comply with applicable privacy provisions of state and federal laws, including the Health Insurance Portability and Accountability Act (HIPAA). Ways in which a provider can protect member/patient PHI include ensuring that only authorized provider office employees have access to member/patient charts, including limited information on member/patient sign-in sheets and restricting non-employees from being in areas of the office that contain member/patient records.

HIPAA Security

The HIPAA Security Rule requires covered entities to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (e-PHI) that is collected, maintained, used, or transmitted by a covered entity. As a covered entity, you must ensure that you have the appropriate administrative, technical, and physical safeguards in place to protect the data that is being electronically accessed by our workforce. You must (a) ensure the integrity and confidentiality of the information; and (b) protect against any reasonably anticipated (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information. This can be accomplished by establishing appropriate policies and procedures that outline your compliance with the Rule and your expectations of your workforce in complying with the Rule. Compliance with the Security Rule is not a one-time goal; it is an ongoing process that requires periodic risk analyses and audits of covered entities' employees' devices to confirm their compliance with your established policies.

A member's PHI must be safeguarded, and only those employees of the covered entity who have a business need to access the information should be permitted to do so. Access to member PHI should be role-based. This means that access should only be granted to a covered entity's employees based on their job duties and responsibilities within the organization.

Healthfirst Compliance Program

To report suspected fraud and abuse or other violations of company policy, call **1-877-879-9137** or go to **www.hfcompliance.ethicspoint.com**

©2016 HF Management Services, LLC.

1958