CENTERS for MEDICARE & MEDICAID SERVICES

CENTER for PROGRAM INTEGRITY

Medicare Advantage and Part D

FRAUD HANDBOOK

Practical Techniques and Approaches on Detecting and Preventing Fraud

Version 1.0 March 2014

CONTENTS

1. PURPOSE OF HANDBOOK AND INSTRUCTIONS FOR USE

This handbook is designed to inform sponsors about detecting and preventing fraud in Medicare Part C (Medicare Advantage) and Part D (Prescription Drug Benefit Program).

1.1. Scope and Purpose

This handbook is a modular, online reference providing sponsors with industry best practices regarding processes, methods, and resources to support fraud prevention, detection, corrective action, preliminary investigation, and referral activities. Its purpose is to serve as a basic reference, with a focus on practical techniques and approaches.

1.2. Audience

This handbook is for Medicare Part C and Part D sponsor personnel involved in anti-fraud initiatives, including:

- Executives
- Compliance officers
- Compliance staff
- Fraud, waste, and abuse (FWA) staff
- Investigative staff

The content below assumes you have an in-depth knowledge of Medicare Part C and Part D, as well as of your own sponsor's service offerings.

1.3. Objectives

Using this handbook will enable you to:

- Demonstrate understanding of the critical success factors of an anti-fraud program and be able to evaluate internal organizational structures, policies, controls, and reporting to determine need for change
- Understand and comply with federal laws and regulatory requirements on preventing, detecting, and correcting fraud
- Recognize and identify fraud vulnerabilities and risks in Medicare Part C and Part D
- Apply basic analytic tools for detecting potential fraud
- Apply basic tools for investigating potential fraud

- Demonstrate understanding of how to report and refer suspected cases of fraud
- Identify the kinds of case support required to support successful prosecution and recovery
- Develop an effective fraud-prevention program

1.4. Definitions

The following definitions apply to the information presented in this handbook and, unless otherwise noted, are the definitions used in CMS's Compliance Program Guidelines, issued as Chapter 9 of the "Prescription Drug Benefit Manual" (PDBM) and Chapter 21 of the "Medicare Managed Care Manual" (MMCM). Both chapters are identical and apply equally to Part C and Part D plans, and we will collectively refer to these chapters as the "Compliance Program Guidelines" in this handbook. See the Appendix of this handbook for the definitions of acronyms.

Abuse: This 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 get paid. 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.

Audit: This is a formal review of compliance with a particular set of standards (e.g., policies and procedures, laws and regulations) used as base measures. (Also see "external audit" and "internal audit.")

Beneficiary: An individual who is entitled to or enrolled in Medicare Part A (Hospital Insurance) or enrolled Part B (Supplementary Medical Insurance) or both under title XVIII of the Social Security Act. For the purpose of this handbook, "beneficiary" is used interchangeably with "enrollee" in Medicare Part C and/or Part D.

Compliance Program Guidelines: As noted in the introduction to this section above, "Compliance Program Guidelines" in this handbook refers to Chapter 9 of the PDBM and Chapter 21 of the MMCM. Both chapters are identical and apply equally to Part C and Part D.

CMS NBI MEDIC: The National Benefit Integrity (NBI) Medicare Drug Integrity Contractor (MEDIC) is an organization CMS has contracted to perform specific program integrity functions for Part C and Part D under the Medicare Integrity Program. The NBI MEDIC's primary role is to identify potential fraud, waste and abuse (FWA) in Medicare Part C and Part D.

Data analysis: This is a tool used to identify coverage and payment errors and other indicators of potential FWA and non-compliance.

Downstream entity: Any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the Part C or Part D benefit, below the level of the arrangement between a Part C

sponsor or applicant or a Part D 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.[1]

Employee(s): Persons employed by the sponsor or a First-Tier, Downstream, or Related Entity (FDR) and who provide health or administrative services for an enrollee.

Enrollee: A Medicare beneficiary who has signed up for a sponsor's Medicare Part C or Part D plan.

External audit: An audit of the sponsor or its FDRs conducted by outside auditors, not employed by, or affiliated with, and independent of, the sponsor.

First-tier entity: Any party that enters into a written arrangement, acceptable to CMS, with a Part C or Part D sponsor or applicant to provide administrative services or healthcare services to a Medicare eligible individual under the Medicare Part C or Part D program.[2]

Formulary: The entire list of Part D drugs covered by a Part D plan and all associated requirements outlined in Pub. 100-18, Medicare PDBM, Chapter 6.

Fraud: Knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any healthcare 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 healthcare benefit program.

Governing body: The group of individuals at the highest level of governance of the sponsor, such as the board of directors or the board of trustees, who formulate policy and direct and control the sponsor in the best interest of the organization and its enrollees. As used in this handbook, the governing body does not include C-level management such as the chief executive officer, chief operations officer, chief financial officer, unless persons in those management positions also serve as directors or trustees or otherwise at the highest level of governance of the sponsor.

High Risk Area (HRA): Geographical areas CMS designates as high risk due to emerging or widespread anomalies that may lead to potential fraud and abuse in, for example, Part C or Part D enrollment.

Internal audit: An audit of the sponsor or its FDRs conducted by auditors who are employed by or affiliated with the sponsor.

Medicare: The national health insurance program for the following:

- People 65 or older
- People under 65 with certain disabilities
- People of any age with End-Stage Renal Disease (ESRD) (permanent kidney failure requiring dialysis or a kidney transplant)

[1] 42 CFR § 423.501

[2] 42 CFR § 423.501

Monitoring activities: Regular review performed as part of normal operations to confirm ongoing compliance and to ensure that corrective actions are undertaken and effective

Office of Inspector General (OIG) (within HHS). The HHS OIG is responsible for audits, evaluations, investigations, and law enforcement efforts relating to HHS programs and operations, including the Medicare program.

Pharmacy Benefit Manager (PBM): An entity that provides pharmacy benefit management services, which may include contracting with a network of pharmacies; establishing payment levels for network pharmacies; negotiating rebate arrangements; developing and managing formularies, preferred drug lists, and prior authorization programs; performing drug utilization review (DUR); and operating disease management programs. Some sponsors perform these functions in-house and do not use an outside entity as their PBM. Many PBMs also operate mail-order pharmacies or have arrangements to include prescription availability through mail-order pharmacies. A PBM is often a first-tier entity for the provision of Part D benefits.

Related entity: Any entity that is related to a Part C or Part D sponsor by common ownership or control that (1) performs some of the sponsor's management functions under contract or delegation; (2) furnishes services to Medicare enrollees under an oral or written agreement; or (3) leases real property or sells materials to the sponsor at a cost of more than $2,500 during a contract period.[3]

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

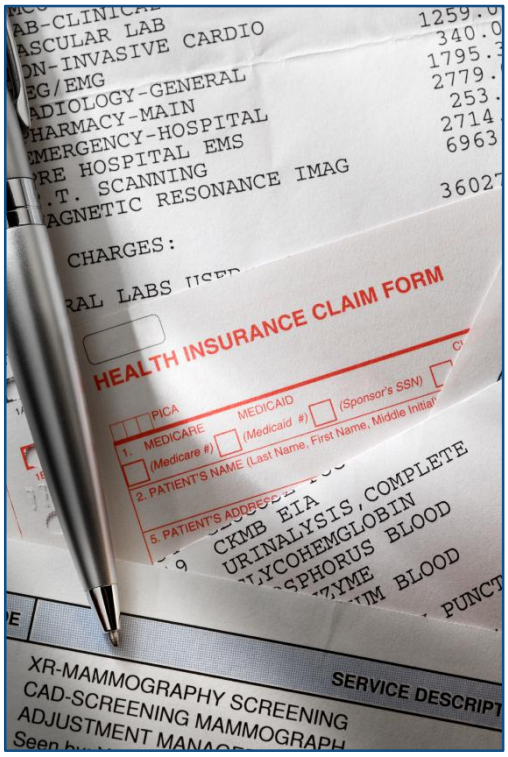
Sponsor: A private organization that sponsors a Medicare Part C or Part D plan.

Waste: The overuse 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.

Whistleblower (also known by the legal term "relator"): This is an employee, former employee, or member of an organization who reports suspected misconduct to people or entities that have the power to take corrective action.

[3] 42 CFR § 423.501

2. FRAUD BASICS



Healthcare fraud is a rising threat, with national healthcare spending topping $2.7 trillion in 2012. Rooting out fraud in healthcare is one of the Federal Bureau of Investigation's top criminal priorities. Medicare programs are particularly vulnerable because of their complexity, improper payment rates, and size. For this reason, the U.S. Government Accountability Office (GAO) designated Medicare a "high-risk program" in 1990.[4]

Many forms of healthcare fraud and abuse pose a threat to the health and safety of countless Americans, including many of the most vulnerable members of our society. To respond to this serious problem, Congress passed, and the President signed into law, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA required the Attorney General of the United States and the Secretary of the Department of Health and Human Services (HHS), acting through the Inspector General, to establish a coordinated national Health Care Fraud and Abuse Control (HCFAC) program. The HCFAC program provides a coordinated framework for federal, state, and local law enforcement agencies; the private sector; and the public to fight healthcare fraud. Examples of the fraud that is being addressed through HCFAC are described below.[5]

- **Organized criminal enterprises**: The Department of Justice (DOJ) Criminal Division's Organized Crime and Gang Section (OCGS) supports the investigations and prosecutions of fraud targeting the 2.5 million private sector plans, as well as investigations and prosecutions of healthcare frauds perpetrated by domestic and international organized crime groups. In FY 2012, the OCGS increased the number of attorneys assigned to healthcare fraud prosecutions, despite substantial budget limitations.[6]
- **Sham operations**: Individuals with program or technical knowledge but no ties to criminal enterprises that, for example, set up fake health services clinics or pay a small fee to sign on as suppliers of medical equipment and then submit bills without ever seeing an enrollee or providing services.

---

[4] GAO, GAO's 2013 High-Risk Update: Medicare and Medicaid (Washington, DC, 2013), 1. Accessed Aug. 6, 2013, at http://www.gao.gov/assets/660/652386.pdf.

[5] HHS and DOJ, The Department of Health and Human Services and the Department of Justice Health Care Fraud and Abuse Control Program Annual Report For FY 1997 (Washington, DC, January 1998), 3-4. Accessed Aug. 6, 2013, at http://oig.hhs.gov/publications/docs/hcfac/hcfacreport1997.PDF.

[6] HHS and DOJ, The Department of Health and Human Services and The Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2012 (Washington, DC, February 2013), 85. Accessed Aug. 6, 2013 at http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2012.pdf.

- **Pharmaceutical and device manufactures:** Companies using marketing schemes to make false and misleading statements about safety or unapproved uses that do not qualify for coverage under federal healthcare programs.

While the vast majority of healthcare professionals are honest, fraud perpetrators threaten the integrity and solvency of Medicare and other federal healthcare programs. Detecting and preventing this fraud is essential to maintaining a healthcare system that is affordable for everyone.

As a sponsor professional charged with safeguarding Part C and Part D programs, you are responsible for recognizing activity that may be considered criminal conduct, fraud, waste, or abuse. This chapter introduces you to the differences between fraud, waste, and abuse; the laws addressing healthcare fraud; and common types of fraud.

2.1. Legal Elements of Healthcare Fraud

As noted in Section 1.4., the definition of fraud used in the Compliance Program Guidelines is:

> Knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any healthcare 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 healthcare benefit program.

It is important to note, however, many legal definitions of fraud exist. Each contain different legal elements. Some of these elements include:

- Intentional deception or deliberate omission
- Knowledge of the falsity of the misrepresentation or ignorance of its truth
- A victim relying on the misstatements
- Damage to the victim
- Wrongful gain to the perpetrator

Fraud?

The gender of enrollees has no impact on a claims reviewer's decision to pay for their flu shots. So if a sponsor routinely misstates enrollees' gender on flu shot claims, it is not fraud.

Fraud

A man's personal and family medical history does affect a claims reviewer's decision to pay for colonoscopy services once every two years. So it is fraud if the personal and family histories are intentionally misstated and claims reviewers authorize paying for colonoscopy services once every two years falsely believing the enrollees are at a high risk for colorectal cancer.

If you can prove these elements, you can prove fraud beyond a reasonable doubt in criminal proceedings. "Beyond reasonable doubt" is the highest standard used as the burden of proof. In some scenarios, however, your evidence may not meet the standard of beyond a reasonable doubt but may be sufficient to prove by "a preponderance of the evidence" for a civil judgment.

2.2. Healthcare Fraud Laws

A number of laws address healthcare fraud. These laws establish the framework for the prosecution of criminal acts and the initiation of civil suits by injured parties. The text that follows explains a number of these applicable laws, including the Federal False Claims Act and the related Whistleblower (Qui Tam) Protection, the Federal Anti-Kickback Statute, the Affordable Care Act of 2010, the Physician Self-Referral Prohibition Statute (Stark Law), and the Beneficiary Inducement Law.

2.2.1. Federal False Claims Act

The Federal False Claims Act is a federal law that makes it a crime for any person or organization to knowingly make a false record or file a false claim to any program funded directly, in whole or in part, by the federal government. The Federal False Claims Act is the primary federal law used to fight Medicare fraud. It has become one of the most widely enforced statutes to fight healthcare fraud.

More specifically, the Federal False Claims Act applies to any person or organization that does any of the following:

- Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval to a federal government employee
- Knowingly makes, uses, or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the federal government
- Conspires to get a false or fraudulent claim allowed or paid to defraud the federal government
- Knowingly makes, uses, or causes to be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money to the federal government
- Acts in deliberate ignorance of the truth or falsity of the information
- Acts in reckless disregard of the truth or falsity

Examples of Federal False Claims Act Violations

Billing for items or services not provided: Submission of a claim for healthcare services, treatments, diagnostic tests, medical devices, or pharmaceuticals that were never rendered.

Ghost patients: Submission of a claim for healthcare services, treatments, diagnostic tests, medical devices, or pharmaceuticals provided to a patient who either does not exist or who never received the service or item billed for in the claim.

Unbundling: Many health plans have special reimbursement rates for groups of procedures typically performed together, such as laboratory tests. One common type of fraud has been to "unbundle" these procedures or tests and bill each one separately, resulting in greater reimbursement than the bundled reimbursement rate.

Improperly coded claims/"upcoding": Submission of a claim coded to a covered medical service when the actual service provided would not be covered. Also, a claim upcoded to pay for a more specialized service or one involving more time or complexity when the service provided was actually general in nature or did not require a specialized level.

The Federal False Claims Act imposes two types of liability:

- The submitter of the false claim or statement is liable for a civil penalty, regardless of whether the submission of a claim actually causes the government any damages and even if the claim is rejected
- The submitter of the claim is liable for damages that the government sustains because of the submission of the false claim

Under the Federal False Claims Act, those who knowingly submit or cause another person to submit false claims for payment by the government are liable for three times the government's damages plus civil penalties of $5,500 to $11,000 per false claim.

2.2.2. Whistleblower (Qui Tam) Protection

The Federal False Claims Act includes a "qui tam" provision that allows people who are not affiliated with the government to file actions on behalf of the government (called "whistleblowers" informally or "relators" per the legal term). Persons filing under the Federal False Claims Act stand to receive a portion (between 15 to 30%, depending on the circumstances of the case) of any recovered damages.

Whistleblower/Qui Tam

Whistleblower (also known by the legal term "relator"): An employee, former employee, or member of an organization who reports suspected misconduct to people or entities that have the power to take corrective action.

Qui tam: An action to recover a penalty under a statute that gives part of the penalty to the whistleblower and the rest to the state or a public body.

The provision also protects employees who file a Federal False Claims Act qui tam case from discharge, demotion, suspension, threats, harassment, and discrimination in the terms and conditions of their employment. Whistleblower employment protection under the 1986 Federal False Claims Act Amendments includes reinstatement with seniority status, special damages, and double back pay.

2.2.3. Federal Anti-Kickback Statute

The Federal Anti-Kickback Statute makes it a felony for healthcare professionals, entities, and vendors to knowingly offer, pay, solicit, or receive remuneration of any kind to induce or reward referrals of business under a federal healthcare program. Remuneration, under the Federal Anti-Kickback Statute, includes the transfer of anything of value, directly or indirectly, overtly or covertly, in cash or in kind.

Fee Splitting

Under the Federal Anti-Kickback Statute, "fee splitting" is a felony. Fee splitting occurs when one provider shares a fee with another for getting a referral.

The Federal Anti-Kickback Statute does not require specific intent: To be in violation of the Federal Anti-Kickback Statute, a person:

- Must have acted with general knowledge that conduct was wrongful
- Need not have acted with specific intent to violate the Federal Anti-Kickback Statute

Persons found guilty of violating the Federal Anti-Kickback Statute may be subject to a fine of up to $25,000, imprisonment of up to five years, and exclusion from participation in federal healthcare programs for up to 1 year. They may also face costly civil penalties and possible prosecution under many similar state laws.

Federal Anti-Kickback Statute Safe Harbors

Managed Care Price Reductions Safe Harbor

- Must be a contract (e.g., fee for service, monthly capitated payment) between a provider and the Part C sponsor for the sole purpose of furnishing covered items and services to Part C enrollees
- Minimum one-year agreement
- The fee schedule must remain in effect throughout the term of agreement
- Covered items/services and payment requirements must be set in advance
- The cost report must show amount paid
- Neither party can induce traditional Medicare business or shift the financial burden of the agreement to the traditional Medicare program
- It does not cover payments for marketing or other non-clinical services bundled with medical services

Discount Safe Harbor

- Invoices must show a price concession
- Price reduction must be fixed at the time the sale is made (even if payment is made later)
- If a buyer is required to submit cost reports to CMS, the buyer must disclose the price concessions on them
- Compensation is fair market value
- Compensation is unrelated to the volume or value of referrals

Important Change

The Affordable Care Act made Federal Anti-Kickback Statute violations automatically false claims for Federal False Claims Act purposes. The Affordable Care Act also revised the evidentiary standard under the Federal Anti-Kickback Statute, eliminating the requirement of actual knowledge of, or specific intent to commit, a violation of the statute. Accordingly, providers will not be able to successfully argue that they did not know they were violating the Federal False Claims Act because they were not aware the Federal Anti-Kickback Statute existed. For more information on the Affordable Care Act, please see Section 2.2.4. below. For more information on the Federal False Claims Act, please see Section 2.2.1.

2.2.4. Affordable Care Act of 2010

The Patient Protection and Affordable Care Act of 2010 (PPACA) and Health Care and Education Reconciliation Act of 2010—together known as the Affordable Care Act—strengthened healthcare fraud and abuse detection and prevention. The Affordable Care Act, among other things, created new healthcare fraud enforcement tools, made it easier for the government to recapture any funds acquired through fraudulent practices, made obstructing a fraud investigation a crime, and increased the federal sentencing guidelines for healthcare fraud offenses by 20 to 50% for crimes involving more than $1 million in losses.

The Affordable Care Act also authorized stronger civil and monetary penalties for persons who knowingly:

- Order or prescribe a medical or other item or service during a period in which the person was excluded from a federal healthcare program when the person knows or should know that a claim for the item or service will be made under the program
- Make or cause to be made any false statement, omission, or misrepresentation of a material fact in any application, bid, or contract to participate in or enroll as a provider of services or a supplier under a federal healthcare program
- Fail to report and return an overpayment within specified time limits
- Fail to grant the HHS OIG timely access (upon reasonable request) for the purpose of audits, investigations, evaluations, or other statutory functions
- Make or use a false record or statement material to a false or fraudulent claim for payment for items and services furnished under a federal healthcare program

Anyone who engages in these activities may also face exclusion from participation in federal healthcare programs.

2.2.5. Physician Self-Referral Prohibition Statute (Stark Law)

The Physician Self-Referral Prohibition Statute contains three provisions commonly referred to as the "Stark Law," which prohibits doctors from referring Medicare and Medicaid patients for certain designated health services to an entity with which the doctor or a member of the doctor's immediate family has a financial relationship, unless an exception applies.

Prohibited Referrals

Doctors cannot refer Part C patients to a medical equipment supply store, pharmacy, or other entity they or a family member owns, with few exceptions. Doctors are also prohibited from accepting "referral fees" in exchange for their advice.

It also prohibits an entity from presenting or causing to be presented a bill or claim to anyone for designated health services furnished as a result of a prohibited referral.

The following items or services are designated healthcare services:

- Clinical laboratory services
- Physical therapy services
- Occupational therapy services
- Outpatient speech-language pathology services
- Radiology and certain other imaging services
- Radiation therapy services and supplies
- Durable medical equipment and supplies
- Parenteral and enteral nutrients, equipment, and supplies
- Prosthetics, orthotics, and supplies
- Home health services
- Outpatient prescription drugs
- Inpatient and outpatient hospital services.

Anyone found guilty of violating the Stark Law faces

- A monetary penalty of up to $15,000, and in certain cases, up to $100,000, for each violation
- Exclusion from participating in Medicare and Medicaid programs

2.2.6. Beneficiary Inducement Law

The federal healthcare program Beneficiary Inducement Law, created in 1996 as part of HIPAA, makes it illegal to offer an exchange of remuneration that a person knows or should know is likely to influence a beneficiary to select a particular provider, practitioner, or supplier. This includes:

- Offering payments or gifts to induce enrollees to come in for a consultation or treatment
- Waiving co-payments and deductibles to induce enrollees to receive services from a provider

Allowable Gratuities

Items and services offered to beneficiaries for free must be worth less than $10 and total less than $50 per year per beneficiary. Cash or gift cards can never be given to beneficiaries.

Anyone found in violation of this law is issued a civil monetary penalty — up to $10,000 for each wrongful act. Penalties can be assessed up to three times the amount claimed. Violators may also be excluded from participating in Medicare and Medicaid programs.

2.3. Medicare Part C and Part D Fraud Schemes

Fraud schemes are limited only by the imagination of people looking to cheat Part C and Part D sponsors, the government, and U.S. taxpayers. Fraud perpetrators are constantly looking for new and creative ways to exploit each part of a sponsor's daily operations for illicit gain. Fraud perpetrators can range from criminal enterprises to enrollees and their caretakers to a sponsor's FDRs. FDRs can include doctors, pharmacists, hospitals, radiology and other kinds of clinics, medical and laboratory equipment suppliers, billing agencies, and claims processing firms. Often, various combinations of these individuals and entities are involved in a fraud scheme.

First-Tier, Downstream, and Related Entities (FDRs) Defined

Who are the first-tier, downstream, and related entities?

A **first-tier entity** is any party that enters into a written arrangement, acceptable to CMS, with a Part C or Part D sponsor or applicant to provide administrative services or healthcare services to a Medicare-eligible individual under the Medicare Part C or Part D program. Examples include allied providers, contracted hospitals, and in most cases Pharmacy Benefits Managers (PBMs).

A **downstream entity** is any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the Part C or Part D benefit, below the level of the arrangement between a Part C sponsor or applicant or a Part D sponsor or applicant and a first-tier entity. These written arrangements continue down to the level of the ultimate provider of both healthcare and administrative services. Examples include pharmacies, marketing firms, claims-processing firms, quality assurance companies, and billing agencies.

A **related entity** is any entity that is related to a Part C or Part D sponsor by common ownership or control, and (1) performs some of the sponsor's management functions under contract or delegation; (2) furnishes services to Part C or Part D enrollees under an oral or written agreement; or (3) leases real property or sells materials to the sponsor at a cost of more than $2,500 during a contract period. An example of a related entity would be one in which a sponsor is the parent company of its own in-house PBM.

The text that follows details several broad categories of fraud schemes typically used to defraud Medicare Part C and Part D sponsors. Many individual fraud schemes fall into more than one category. Because new fraud schemes are constantly emerging, the following list is not all-inclusive.

Why Fraudulent Billings under Part C and Part D Matter

Even though Part C and Part D sponsors receive fixed monthly capitated payments to care for their enrollees, any fraudulent claims they pay directly threaten Medicare's integrity and solvency.

Through a mechanism known as "risk adjustment," sponsors receive larger monthly capitated payments to care for enrollees with high risk scores. Risk adjustment is meant to ensure that sponsors are paid fairly but do not benefit from "cherry picking," or disproportionately enrolling the healthiest individuals. When their enrollees' care is in any way touched by fraud, these enrollees' risk scores can become artificially inflated.

It is unclear the role the various fraud schemes described in Section 2.3. play in inflating Part C and Part D monthly capitated payments overall. What is known is that sponsors' diagnostic coding practices cause risk scores for their enrollees to be higher than those for comparable beneficiaries in traditional Medicare. The U.S. General Accounting Office (GAO) found this to be true for 2010, 2011, and 2012. This practice led to, in GAO's words, "inappropriately high MA [Medicare Advantage] risk scores and payments to MA organizations."

For this reason, Part C is expected to cost 104% more this year per beneficiary than traditional Medicare, according to the Medicare Payment Advisory Commission—Congress' expert advisory body on Medicare payment policy.

2.3.1. Services Not Rendered

One of the most obvious examples of healthcare fraud is the submission of claims for services that were never delivered to enrollees. In some cases, a lack of quality of care equates to services not rendered. This basic scheme has many variations:

- The submission of claims for services that were never performed, medical supplies and equipment that were never delivered, lab or medical tests that never occurred, or prescriptions that were never filled. These schemes can involve identity theft (see Section 2.3.5.), kickbacks (see Section 2.3.7.), and collusion between licensed doctors and fake healthcare entities. They can also involve falsifying enrollee records with non-existent symptoms to make it appear that enrollees required services, tests, supplies and equipment, or drugs.
- The theft or purchase of doctor and patient data to carry out schemes similar to the ones noted above. Under these schemes, criminals may open false-front offices that appear to be medical offices from the outside. However, these offices do not provide actual medical care and exist for

the sole purpose of stealing money from sponsors. In similar schemes, criminals use a private mailbox facility as the fraudulent medical office address, with the entity's mailbox number as its "suite" number.

- The operation of "rolling labs" located at places such as health clubs, retirement homes, and shopping malls and that provide fake tests given to Part C and Part D enrollees and billed to the sponsors.
- Enrollees or their caretakers allowing the submission of bills for undelivered procedures, equipment, or services in exchange for cash, drugs, or other inducements.
- Enrollees submitting false reimbursement claims for non-existent out-of-pocket expenses for drugs and medicines.
- Providers or third-party billers adding charges for undelivered procedures or services to a bill for legitimate charges.
- Providers submitting claims for services, treatments, diagnostic tests, medical devices, or pharmaceuticals for enrollees who are deceased.
- Home health agencies submitting claims for home health services for enrollees whose records show them hospitalized on the service dates.
- Providers or sponsors pocketing monthly capitation payments while providing inaccessible or inadequate enrollee care. Examples include denying needed treatment by withholding proper medical evaluation; substituting providers without the necessary medical credentials; failing to have enough providers to meet the needs of the enrolled populations; or requiring enrollees to use a provider whose office is far from their homes, has limited office hours, has long waiting times for appointments, or whose office is hard to reach using public transportation.
- Providers billing for a higher level of services than was actually provided to get a fraudulently higher level of reimbursement. Examples include providing home health aides and billing for professional nursing staff or providing basic physical therapy and billing for aqua-therapy.
- Providers continuing to bill for a product after an enrollee has returned the equipment, has discontinued use of equipment or supplies (such as oxygen), or has refused to accept delivery.
- Pharmacists dispensing prescriptions a few pills short or misrepresenting the quantity of injectables dispensed (e.g., billing for syringes that are routinely boxed in multiple sets as single syringes).
- Pharmacists billing for prescriptions that enrollees failed to pick up.

2.3.2. Lack of Medical Necessity

One of the least obvious examples of healthcare fraud is filing claims for care that in no way applies to the condition of an enrollee. This basic scheme can range from claims for unnecessary procedures or diagnostic tests bundled with claims for legitimate ones or claims for expensive therapies, surgeries, home health services, or equipment the enrollee's condition does not require. Often the therapies and treatments are not provided, and the drugs involved are resold illegally as part of controlled substances schemes (see

Section 2.3.6.). These schemes can involve patient "recruiters" who identify enrollees who will cooperate by going to a fake clinic to meet with a physician in collusion with the scheme. This physician then documents non-existent conditions and prescribes treatments and drugs that are billed to the sponsor. Colluding enrollees often receive payments like cash, drugs, and equipment (such as expensive wheelchairs that are resold illegally). Enrollees may be innocent victims or co-conspirators. Caregivers may also be involved in the fraud. As with services-not-rendered schemes, these types of schemes can involve kickbacks (see Section 2.3.7.) and false patient records with non-existent symptoms to make it appear that the enrollees required the services, tests, supplies and equipment, or drugs.

2.3.3. Services Misrepresented

Claims misrepresenting the actual services provided are another category of fraud. This basic scheme takes several forms:

- Providers falsely billing for a covered medical service when the actual service provided would not be covered. An example is massage, which is not covered, as opposed to physical therapy.
- Colluding enrollees receiving free housecleaning, groceries, spa services, dance classes, and various other non-reimbursable services and promising to acknowledge they received the actual services billed if ever asked. Typically, these schemes involve recruiters who provide kickbacks to enrollees they meet at such places as retirement communities, civic group meetings, or government program offices (also see Section 2.3.7.).
- Misleading enrollees who are not in on a scam about receiving free housecleaning, groceries, and various other non-reimbursable services. These schemes also typically involve recruiters, but in these cases, the recruiters mislead enrollees into believing they can receive free services under their health coverage just by providing the recruiter with their enrollee member identification number. The recruiter then uses the enrollee's identification number to submit false claims for different services or for services that were never received.

2.3.4. Fraudulent Billing Schemes

Many fraud schemes involve incorrectly coding services on claims. There are many variations of billing schemes:

- **Unbundling**: In many cases, sponsors have special reimbursement rates for groups of procedures typically performed together, such as laboratory tests and pre- and post-operative procedures associated with surgery. One common billing scheme is to unbundle these tests or procedures and bill each one separately, resulting in greater reimbursement than the group reimbursement rate.
- **Upcoding**: Sponsors use a set of billing codes that providers use to bill for services, tests, and supplies. In an upcoding scheme, providers fraudulently use a higher paying code to reflect that more costly procedures, devices, supplies, or tests were involved in the enrollee's treatment. In some cases, third-party billing companies develop automated schemes to upcode common procedures and then split the fraudulent revenues with insiders.
- **Duplicate billing**: A fraudulent provider changes some small portion of a previously submitted claim, such as a date, to charge the sponsor twice for the same service. Alternatively, a fraudulent provider charges both the facility (e.g., emergency room) and the professional (e.g., physician) for an outpatient procedure and then colludes with the medical professional, who bills the professional charge again.
- **Double billing**: A provider bills more than one payer for the same claim, such as Medicare Part A or Part B, Medicaid, a state health insurance program, private insurance, or even the enrollee, who is fraudulently told that the Part C or Part D sponsor does not cover the procedure or prescription.
- **Fragmentation of claims**: A fraudulent provider bills necessary services across several days or encounters that could have been done in fewer days or encounters (e.g., consecutive hospital stay sequences). Or, a fraudulent provider performs several services on the same day but bills them across several claims on different dates of service.
- **Third-party biller scams**: Some schemes involve third-party billers adding claims without providers' knowledge and keeping the reimbursements. The perpetrators can range from office staff to large corporate billing companies.
- **Capitated payment fraud**: A doctor can fraudulently increase the number of diagnoses on an enrollee's chart. These inflated diagnoses are then submitted to the sponsor, which pays a higher monthly fee to the doctor (capitated payment) because the enrollee appears to have a high number of health problems on paper. This scheme is seen in many settings, including acute care and home health where reimbursement rates are higher with more acute diagnoses.

Example of a Common Durable Medical Equipment (DME) Upcoding Scheme

A common scheme is billing a sponsor for a new motorized wheelchair when the patient really received a manual wheelchair, a scooter, or used equipment.

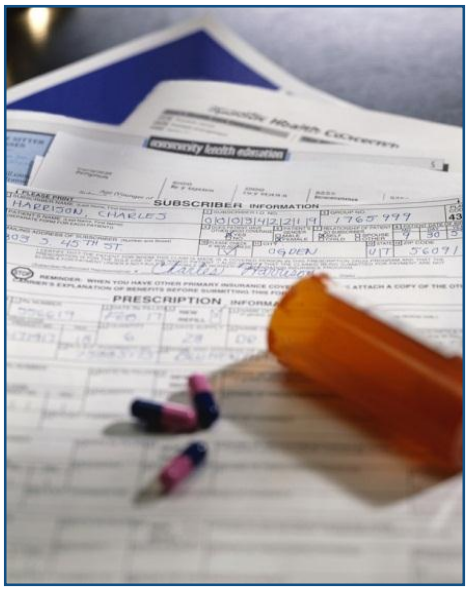
- **Misrepresentation of credentials**: A fraudulent provider submits a false claim misrepresenting the credentials of the person who provided the services. These cases typically involve a provider billing the sponsor as if someone eligible for reimbursement delivered the services, when the person who actually delivered them was precluded from reimbursement (e.g., lacking credentials or being specifically excluded from receiving Medicare reimbursement). These schemes may involve billing with a stolen or colleague's provider identification number or falsely representing that a teaching physician was present for procedures that were provided by a medical school student.
- **Drug pricing fraud**: A fraudulent drug manufacturer misrepresents the number of doses in a container or misrepresents the actual manufacturing costs to charge grossly inflated drug prices.
- **Partial prescription fills**: A fraudulent pharmacy fills a partial month's drug supply and asks the beneficiary to come back for the rest. The pharmacist then bills the sponsor twice in one month for the full amount.
- **Shorting**: A fraudulent pharmacy bills for a larger quantity of a drug than it provided to the beneficiary.
- **Drug switching**: A fraudulent pharmacy bills for a name brand drug but supplies the beneficiary with a generic drug.
- **Thin air scripting (services not rendered combined with identity theft)**: A fraudulent pharmacy bills a sponsor for prescriptions that a doctor never prescribed or the beneficiary never received.

2.3.5. Identify Theft

Identity theft is another type of healthcare fraud taking many forms:

- Telemarketers using "phishing" techniques to trick enrollees into providing their identification numbers for fraudulent purposes. These schemes are particularly numerous and can involve offers for "free" services, tests, equipment, or even cookbooks that require a sponsor number to receive. Typical schemes include special offers under a Part D sponsor that will provide a year's supply of prescription drugs for one payment of $299, $389, or $399; motorized wheelchairs for simply calling a "toll-free" number; or a package of home health visits for a fixed price.
- Individuals forging doctors' signatures and prescriptions or stealing provider identification numbers and enrollees' sponsor identification numbers to carry out services-not-rendered schemes (see Section 2.3.1.) or controlled substances schemes (see Section 2.3.6.).
- Individuals without healthcare credentials stealing a provider's identification number and using it to submit false claims without the real provider's knowledge. Under these schemes, the scam artist may also change the address of the provider's service location or add additional service locations to have funds diverted.

- Employees of healthcare entities selling enrollees' identification numbers and other personal information to criminals to use for fraudulent purposes, including filing false tax returns to get refunds fraudulently.



- Providers allowing people precluded from reimbursement to use their provider identification numbers to submit false claims.
- Employers using the provider identification numbers of former employees to submit false claims without their consent or knowledge.
- Fraud perpetrators pretending to offer providers jobs to trick them into giving their provider identification numbers. The fraud perpetrators then tell the providers the jobs are no longer available and begin submitting false claims using the providers' identification numbers without their consent or knowledge.
- Doctors allowing criminals to use their prescription pads to write fraudulent prescriptions for narcotics and other drugs.
- Enrollees or criminals stealing physician Drug Enforcement Agency (DEA) numbers, prescription pads, or e-prescribing log-in information to get medications fraudulently.
- Uninsured individuals in need of medical care using the sponsor identification number of someone with coverage. In some cases, sponsor identification numbers are stolen. In others, beneficiaries let people borrow their identification numbers as a favor or for payment.

2.3.6. Controlled Substances Schemes

Schemes involving controlled substances are of significant concern in all federal healthcare programs. In some areas of the country, Schedule II prescription painkillers like oxycodone are more common street drugs than illegal drugs, such as cocaine. Controlled substances schemes take several forms:

- **Pill mills**: Separate healthcare individuals and entities — usually including a pharmacy — collude to generate a flood of fraudulent prescriptions. In some schemes, the enrollee sells the filled prescription to pill buyers who either sell them on the street or back to the pharmacy. In other schemes, the enrollees are "drug seekers" who are given prescriptions for controlled substances without any legitimate medical purpose for the prescriptions. In these cases, they pay the prescribing doctor kickbacks.

- **Prescription harvesting**: Criminals steal, buy, or trick enrollees into giving them identification numbers (see Section 2.3.5.) and then bill sponsors for a flood of expensive drugs and controlled substances. These dispensed drugs never reach the enrollees. Instead, they are diverted to pill buyers who either sell them on the street or back to pharmacies.
- **Shorting**: A pharmacy routinely dispenses prescriptions a few pills short and then keeps the extra pills to sell again later to regular customers or pill buyers. Pill buyers will sell them on the street or back to pharmacies.
- **Double billing**: A pharmacy informs enrollees that certain prescriptions are not covered by their sponsor. After the enrollees pay for the prescriptions out of pocket, the pharmacy bills the sponsor for the same prescriptions.
- **Doctor or pharmacy shopping**: Enrollees get multiple prescriptions for controlled substances (usually Schedule II prescription painkillers, such as oxycodone) from multiple doctors and pharmacies. Law enforcement agencies call these individuals "Drug-Seeking Beneficiaries" or "benes" (DSBs).
- **Enrollee forgery**: Enrollees alter prescriptions (e.g., changing the quantity from 30 to 130) or steal doctors' DEA numbers, prescription pads, or e-prescribing log-in information to get prescriptions fraudulently.

Drug and Other Substances Schedules

The Drug Enforcement Administration and Food and Drug Administration categorize drugs and other substances into schedules regulating their manufacture, importation, possession, use, and distribution. Drugs and other substances are:

- **Schedule I:** When they have a high potential for abuse and have no currently accepted medical use in treatment in the United States
- **Schedule II:** When they have a high potential for abuse, and their abuse may lead to severe psychological or physical dependence
- **Schedule III:** When their abuse may lead to moderate or low physical dependence or high psychological dependence
- **Schedule IV:** When their abuse may lead to limited physical or psychological dependence relative to the drugs or other substances in Schedule III
- **Schedule V:** When their abuse may lead to limited physical or psychological dependence relative to the drugs or other substances in Schedule IV

2.3.7. Kickbacks and Self-Referrals

As noted in Section 2.2.3., the Federal Anti-Kickback Statute prohibits providers from accepting remuneration of any kind in exchange for their referrals. As noted in Section 2.2.5., the Doctor Self-Referral Prohibition Statute prohibits doctors from referring patients to an entity with which the doctor or a member of the doctor's immediate family has a financial relationship, unless an exception applies.

More on Illegal Referrals

Even if a provider makes referrals to legitimate healthcare entities in exchange for fee discounts and/or is unaware that kickbacks are prohibited within Part C or Part D sponsors, it is still a felony. This illegal practice is known as a ***pull through scheme***.

Fraud schemes in violation of these statutes take many forms. They include referral fees, discounted pricing to providers or sponsors in exchange for referrals, fee-splitting agreements, finder's fees, marketing fees, discounted leases or equipment rentals, speaker's fees, and free or discounted travel or entertainment. Many involve kickbacks and prohibited referrals to legitimate healthcare entities. Others are part of larger fraud schemes, such as services not rendered (see Section 2.3.1.), lack of medical necessity (see Section 2.3.2), or services misrepresented (see Section 2.3.3.).

2.3.8. Marketing and Enrollment Fraud

According to the *Department of Health and Human Services and the Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2012*, Part C and Part D marketing and enrollment fraud were down in 2012 compared with 2011 but were still being detected.[7] Such prohibited activities include the following:

- A Part C or Part D sponsor advertises to Medicare beneficiaries different benefits, features, or prescription drug co-pays than listed in its CMS-approved marketing materials. As a result, beneficiaries sign up for coverage, not realizing it does not meet their healthcare needs.
- Without a sponsor's knowledge, a Part C or Part D sponsor's downstream vendors, insurance brokers, or providers create their own marketing materials that misrepresent a sponsor's benefits, features, or prescription drug co-pays. As a result, Medicare beneficiaries enroll with a sponsor, not realizing it does not meet their healthcare needs.
- Insurance brokers fail to provide information on Special Needs Plans (SNPs) for Medicare beneficiaries who live in certain institutions (e.g., a nursing home), require nursing care at home, are also eligible for Medicaid, or have specific chronic or disabling conditions (e.g., diabetes, ESRD, HIV/AIDS, chronic heart failure, or dementia). As a result, Medicare beneficiaries with special needs enroll in a plan that does not fit their medical needs and disrupts their continuity of care.
- Downstream vendors or insurance brokers mislead Medicare beneficiaries to get them to enroll with a Part C or Part D sponsor (e.g., telling them to sign up for services because Medicare is

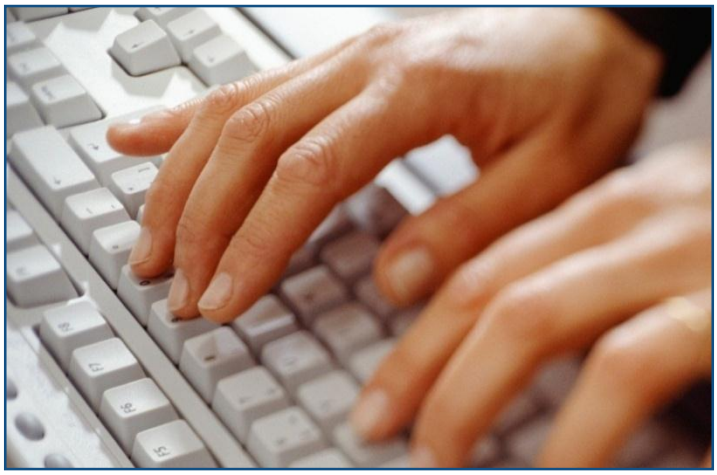
[7] HHS and DOJ, The Department of Health and Human Services and The Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2012 (Washington, DC, February 2013), 62. Accessed Aug. 6, 2013 at http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2012.pdf.

being abolished; misrepresenting a Part C or Part D sponsor's benefits, features, or prescription drug co-pays; or telling them a different sponsor's coverage is free or Medicare endorsed).

- An insurance broker sets up a meeting with a Medicare beneficiary to discuss a Part C or Part D sponsor. The beneficiary provides personal identification, such as name, address, and Social Security number, on a sign-in sheet or card. Without realizing it, the Medicare beneficiary is enrolled with a Part C or Part D sponsor without giving consent.
- A sponsor markets Part C or Part D coverage that CMS has not approved.
- Medicare beneficiaries are invited to a Part C and Part D "educational" event that includes free health screenings or takes place on the second floor of a building without an elevator to "cherry pick" enrollees who are healthy enough to walk a flight of stairs.
- An insurance broker offers incentives, such as meals, trips, or "free" items in return for signing up for Part C or Part D coverage. In related schemes, beneficiaries are told they have to provide their Social Security numbers, current Part C or Part D enrollee identification numbers, and other personal identification information to receive the "free" items, and once they do, they are enrolled in the broker's Part C or Part D plan without their knowledge or consent.

- Insurance brokers collude with administrators of nursing homes and retirement communities to get sole access to the facility to conduct staged marketing presentations. Administrators provide residents' Social Security numbers, current Part C or Part D enrollee identification numbers, and other personal identification information for a fee and then the insurance brokers fraudulently enroll residents in the brokers' Part C or Part D plans without their knowledge or consent.

3. COMBATING FRAUD



To combat Part C and Part D fraud, you first must find it. Many fraud perpetrators are opportunistic and submit false claims in a random manner, making their detection difficult.

Also, Part C and Part D programs are increasingly attracting high-tech, highly skilled, and educated fraud perpetrators who design practically invisible fraud schemes. These highly sophisticated fraud perpetrators study the behavior of sponsors' automated payment systems and fraud detection activities to exploit their predictability. Some experiment relentlessly until they find a successful fraud model and then continually expand it until they are caught — which may take years. Others run very aggressive fraud schemes that swindle sponsors out of millions of dollars in a few days and then quickly shut down. All types will move their operations to new locations or switch to completely new types of scams when sponsors or law enforcement catch onto their schemes.

As a sponsor professional charged with safeguarding Part C and/or Part D programs, you play an important role in determining or implementing the way your organization prevents, detects, and combats fraud. This chapter introduces you to the integrated fraud management life cycle; the federal regulatory requirements mandating that sponsors prevent, detect, and correct fraud[8]; and the staffing and tools you need to implement the integrated fraud management life cycle while complying with regulatory mandates. Each stage of the cycle is also explored in detail in later sections.

3.1. Overview of the Fraud Management Life Cycle

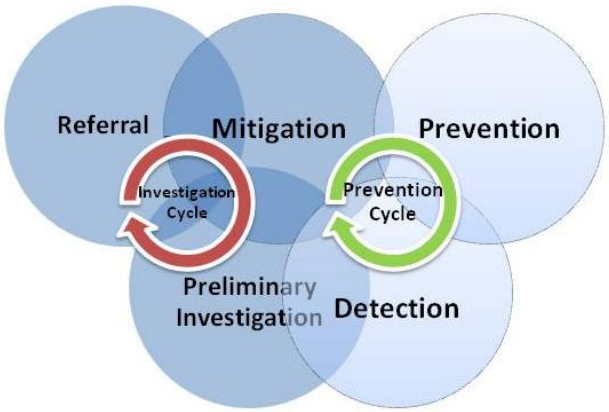
Detecting fraud at the claims stage works well for finding simple false claims. It is less effective, however, in finding other types of fraud, such as:

- Duplicate claims
- Unacknowledged duplicate payments
- Kickbacks and self-referrals
- Marketing and enrollment fraud
- Sophisticated fraud schemes demonstrating great complexity and understanding of sponsor automated payment systems and fraud detection activities

[8] 42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

A far more cost-effective and efficient strategy is including traditional claims investigation in an integrated fraud management life cycle based on both top-down approaches (increasing the difficulty of committing fraud and strengthen the perception that fraud perpetrators will be caught and punished) and bottom-up approaches (promoting institutional integrity and reporting possible fraud). This also may mean "mainstreaming" or integrating anti-fraud functions across business units rather than managing them as "stand-alones." Such an integrated fraud management life cycle is made up of five parts: prevention, detection, corrective action, preliminary investigation, and investigation referral (see Figure 1). These parts are not linear steps; rather, they are concurrent, related processes.

Figure 1: Network Representation of the Fraud Management Life Cycle Stages.



3.1.1. Prevention

To prevent small and massive fraud schemes efficiently and cost effectively, your organization is required, per federal regulations,[9] to implement a Medicare compliance program. Please note, however, that compliance and prevention are not complementary concepts. Because compliance is much broader than fraud management—and entails obeying the law and regulatory requirements in general—it is important to refer to the Compliance Program Guidelines for detailed guidance on establishing and maintaining an effective overall compliance program. The list below details where Medicare compliance program core elements mandated in the federal regulations are discussed in the Fraud Handbook in terms of fraud only:

- Written standards (see Section 4.1.2.)
- Compliance officer and compliance committee (see Section 3.2.1.)
- Training and education (see Sections 4.1.5., 4.2.1., and 4.2.6.)
- Effective lines of communication (see Section 4.2.2.)
- Enforcement of written standards through well-publicized disciplinary standards (see Sections 4.1.2. and 4.1.3.)
- System for routine monitoring and identification of compliance risks (see Section 4.1.4.)
- System to promptly respond to and investigate potential compliance issues (see Sections 3.1.3., 3.1.4., and 3.1.5)

[9]42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

An industry best practice is to include both top-down and bottom-up approaches in your fraud-prevention activities. Top-down prevention occurs at the sponsor's institutional level to create the rules, policies, and procedures necessary for effective fraud prevention. However, for these measures to be successful, sponsors should also take a bottom-up approach to educate and motivate stakeholders, including employees and enrollees, resulting in changed attitudes and behaviors about healthcare fraud.

Top-down approaches increase the difficulty of committing fraud and strengthen the perception that fraud perpetrators will be caught and punished. This includes:

- Written policies, procedures, and standards of conduct to clearly define what is appropriate (see Section 4.1.2.)
- Well-publicized guidelines and enforcement of disciplinary measures, sanctions, and prosecution for fraud perpetrators (see Section 4.1.3.)
- Annual risk assessments, internal and external audits, and monitoring and internal control systems to prevent, detect, and stop fraud (see Section 4.1.4.)
- Outreach programs raising awareness of the top-down approaches above to create the perception that fraud perpetrators will be caught and punished (balanced with messages about the bottom-up approaches described below) (see Section 4.1.5.)

Effective Disciplinary Guidelines

An effective deterrent to provider fraud is having strongly enforced disciplinary guidelines excluding providers from your network in response to all medical board actions, not just suspended or revoked medical licenses. For example, you can require providers be eliminated from your network when their licenses are probated, and then allow them to apply to be reinstated after a certain amount of time following their probationary periods.

Bottom-up approaches promote institutional integrity and a climate in which enrollees and employees actively seek out and report fraud. This includes:

- Training on institutional integrity and federal and state laws against fraud (see Section 4.2.6.).
- Raising employee and enrollee awareness of common fraud schemes and the anonymous reporting tools they can use to report possible fraud in good faith per federal regulations.[10]
- Fostering a work environment where employees feel comfortable reporting possible fraud and may do so anonymously without fear of reprisal, and where they know their concerns will reach the compliance officer and compliance committee (see Section 4.2.2.).

[10] 42 CFR §§ 422.503(b)(4)(vi)(D) and 423.504(b)(4)(vi)(D)

- Offering employees assistance and counseling for alcohol and drug problems, addiction to gambling, marital problems, and financial difficulties. Employee support programs reduce the chance employees in crisis will turn to fraud to make ends meet (see Section 4.2.3.).

Medicare Parts C and D Fraud Work Groups

Medicare Parts C and D Fraud Work Groups, sponsored by CMS, meet quarterly to promote information sharing on the latest fraud schemes.

For more information, please email MEDIC-Outreach@rainmakerssolutions.com.

Another important prevention activity is information sharing, such as participating in the Medicare Parts C and D Fraud Work Groups or collaborating with the Senior Medicare Patrol (SMP), State Health Insurance Assistance Programs (SHIPs), and other Medicare consumer advocacy groups.

For more on prevention activities please see Section 4.

3.1.2. Detection

The second component of an integrated fraud management life cycle is data analytics to detect fraud, including:

- Internal data sources (e.g., enrollee hotline reports, secret shopper findings, internal audit results)
- External data sources (e.g., information shared at Medicare Parts C and D Fraud Work Groups meetings, news reports about fraud schemes)
- Internal and external databases

Low-Cost Data Analysis

Even if you cannot afford state-of-the-art data analytics software, you can identify providers to review for potential fraud by generating simple ratios and matching them provider by provider. Ratios to examine include:

- Average dollars paid per enrollee
- Average dollars paid per medical procedure
- Average medical procedures per visit
- Average visits per enrollee
- Average distance enrollee travels to see provider

If you identify providers who deviate from the norm (e.g., if a provider sees enrollees who on average live 83 miles away when providers in the same specialty in the same area see enrollees who live on average 7 miles away), review further to find out why the provider is deviating so much from the average.

Using a broad range of structural-analysis and pattern-recognition methodologies (to search for patterns of coincidence or clustering across thousands of claims), you can identify fraudulent activity you would never find if you had examined individual claims or patient histories. Your sponsor can also gain a comprehensive view of the fraud perpetrators and FWA schemes within your service area.

Two Part C risks deserve special attention in your data analysis:

- Excluded or deceased providers
- Providers lacking credentials

Three Part D fraud risks deserve special analytic attention:

- Abnormal patterns of prescribing and dispensing
- Missing provider identifiers
- High volume of prescriptions for enrollees outside of the expected geographic area

Urgency vs. Prudence

Ad hoc immediate actions are indeed critical when a sponsor discovers fraudulent activity is taking place within its network, but only temporarily. It is essential to develop, implement, and monitor longer term corrective actions as soon as practicable to address root causes of non-compliance and fraud.

For more on detection activities please see Section 5.

Risk Adjustment Fraud in Part C

Medicare Part C sponsors commit fraud when they knowingly submit risk-adjustment data to CMS using diagnosis codes that are inaccurate or ineligible for payment under CMS rules, such as upcoding enrollee diagnoses to exaggerate the severity of their enrollees' conditions (claiming they are sicker than they really are). This type of fraud improperly increases the amount sponsors receive per month for their enrollees.

3.1.3. Mitigation

Mitigation activities begin when the presence of or a reasonable suspicion of fraudulent activity has been detected. You should begin mitigation activities as quickly as possible. If your detection activities can provide the sponsor with an early warning of the likelihood of a fraud scheme, quick mitigation activities can significantly reduce your organization's losses, expenses, and exposure.

Mitigation activities are part of your organization's program to prevent, detect, and correct FWA and non-compliance with federal regulations.[11] Mitigation activities include:

- Immediate mitigation actions to stop monetary loss and avoid the "pay-and-chase" method of trying to recoup money after paying false claims. Examples include subjecting future claims of prescribers/providers suspected of fraud to pre-payment review, changing the member identification numbers of any enrollees whose identities may have been compromised, or stopping payment of suspect pharmacy claims until you can investigate them and determine they are not fraudulent.

[11] 42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

- Longer term corrective actions addressing root causes to correct fraud promptly and thoroughly, reduce the potential for recurrence, and ensure ongoing compliance with CMS requirements.
- Types of corrective actions to consider for FDRs include warning letters, educational materials, mandated training, procedural changes, payment corrections, and disciplinary action.
- Types of internal corrective actions for sponsors to consider, even when fraudulent activity is limited to an FDR, include revision of prevention activities, revision of detection activities, corrections to erroneous data, enrollee fraud aftercare, payment corrections, and disciplinary action. Taking internal corrective action when fraudulent activity is limited to an FDR will lead to stronger prevention and detection activities (see Sections 3.1.1., 3.2.2., 4, and 5) and move your organization away from piecemeal, reactive engagement toward proactive and preventive engagement.

Commercial Database Use Best Practice

Due to the sensitivity of the information available in commercial databases, you might elect to designate an individual or specific team of individuals to perform these searches. Limiting those with access to commercial databases decreases the likelihood of misuse of this information, such as investigative staff accessing family members' information. Also, if there is a cost per search, limiting the number of employees who can run searches may help contain costs.

An industry best practice is using corrective action plans to correct fraud problems promptly and thoroughly to reduce the potential for recurrence and ensure ongoing compliance with federal regulations.[12] You can require an FDR to develop, implement, and monitor a corrective action plan, as noted above. You can also develop, implement, and monitor an internal corrective action plan to address the issues that enabled fraudulent activity to take place within your network as well as the fraud's aftermath.

Developing such a plan involves eight steps:

- Review of situation
- Root cause analysis
- Identification of corrective actions
- Development of corrective action plan
- Signing of written agreements for any FDRs who engaged in or were associated with suspect behavior
- Implementation of corrective action plan

[12] 42 CFR §§ 422.503(b)(4)(vi)(G)(2) and 423.504(b)(4)(vi)(G)(2)

- Monitoring of corrective action plan
- Addressing non-compliance

For more information on mitigation, please see Section 6.

3.1.4. Preliminary Investigation

In addition to corrective action, a preliminary investigation also begins when the presence or a reasonable suspicion of fraudulent activity has been detected. As required by the Compliance Program Guidelines, sponsors must initiate a reasonable inquiry, including a preliminary investigation, as quickly as possible but not later than two weeks after the date when the potential non-compliance or potential FWA incident was identified. Investigative staff, such as an SIU under the control of your organization's compliance officer (see Section 3.2.2.), help with FWA investigations.

The objective of a preliminary investigation is to determine whether there is a credible allegation of fraud. If a credible allegation of fraud is confirmed, your investigative staff is also responsible for getting enough evidence and information to support corrective action (see Section 3.1.3. and Section 6), providing referral information to the CMS NBI MEDIC and law enforcement, and supporting the successful prosecution and conviction of fraud perpetrators (see Sections 3.1.5. and 8).

A planned, systematic approach for conducting a preliminary investigation includes:

- Developing an investigative plan
- Reviewing statements from anonymous or identified complainants
- Interviewing providers, enrollees, and others
- Conducting a data analytics review of individual complaints for overall patterns, trends, and errors
- Reviewing provider enrollment applications, histories, and ownership; beneficiary enrollment applications; and other documents
- Conducting site visits
- Conducting claims reviews and analysis of records and claims data
- Reviewing medical records
- Reviewing financial and billing information
- Documenting the investigation and preparing case files, assuming an appeals or federal court level of review

If after conducting a reasonable inquiry, your investigative staff determines that potential FWA related to Part C and Part D has occurred, your investigative staff is to promptly make a referral decision (see Sections 3.1.5., below, and 8).

For more information about preliminary investigations, please see Section 7.

3.1.5. Investigation Referral

If the facts discovered during your preliminary investigation lead you to believe a criminal, civil, or administrative law was violated, then the matter should be referred promptly to law enforcement and/or the CMS NBI MEDIC — a CMS-funded investigative group that investigates Part C and Part D FWA cases involving sponsors, pharmacies, providers, or enrollees. You can either:

- Make the CMS NBI MEDIC referral and continue with your investigation — supplemented with CMS NBI MEDIC resources and information (see Section 8.1.5.) — and ongoing communication with the CMS NBI MEDIC until you are done. In this scenario, however, the CMS NBI MEDIC may ask that you not take any further action once law enforcement takes the case.
- Turn the investigation over to the CMS NBI MEDIC within 30 days if you do not have the time or resources to investigate, per the Compliance Program Guidelines at Section 50.7.1.

The CMS NBI MEDIC is funded to refer Part C and Part D FWA cases to law enforcement, through the proper law enforcement channels. The CMS NBI MEDIC reports the case on your sponsor's behalf to CMS, HHS OIG, the FBI, and state or local law enforcement, as appropriate. The CMS NBI MEDIC also provides investigative support to your organization, the OIG, and law enforcement toward the prosecution and conviction of fraud perpetrators.

Your sponsor can report the alleged fraud to CMS, HHS OIG, the FBI, and state or local law enforcement on its own, but it will lose the advantage of CMS NBI MEDIC investigative support — including access to federal databases (see Section 8.1.5.) that could make your case stronger or more appealing to a U.S. Attorney's Office.

During the referral process, each case needs to be treated as if it will be prosecuted — with case files prepared and maintained, assuming an appeal or federal court level of review. This means comprehensive and detailed case documentation, complete detailed descriptions of activities, accurate and complete interview notes, and extensive contact information. It is critical that your investigative staff ensure the integrity of all evidence (e.g., its physical security and its admissibility and usefulness in legal proceedings) by properly documenting, handling, storing, and preserving it. Keeping organized files will also help your investigative staff with information requests from the CMS NBI MEDIC within the typically required 30 days, per the Compliance Program Guidelines in Section 50.7.5.

For more information on referrals, please see Section 8 in this document.

3.2. Necessary Staffing

The staffing needed for your sponsor to prevent, detect, and combat fraud will vary according to the sponsor's size, resources, geography, and managed care and prescription drug plan type. Whatever staffing plan and organizational structure you put in place needs to address all the activities in the fraud management life cycle (see Section 3.1.) as well as federal regulations.[13]

[13] 42 CFR §§ 422.503(b)(4)(vi)(B) and 423.504(b)(4)(vi)(B)

These requirements include designation of a compliance officer and compliance committee and ensuring governing body and senior management oversight. Balancing all fraud management life cycle activities may also mean mainstreaming or integrating anti-fraud functions across business units rather than managing fraud activities as stand-alone units.

Referral to CMS NBI MEDIC

Call the CMS NBI MEDIC at 1-877-7SAFERX (1-877-772-3379). For referral forms, go to healthintegrity.org/docs/NBI_Contract_HI_MEDIC_Complaint_Form_20111109.pdf or healthintegrity.org/docs/HI_MEDIC_Compromised_ID_Report_Form_20120515.pdf.

3.2.1. Personnel-Related Regulatory Requirements

Federal regulations require Part C and Part D sponsors to designate a compliance officer and a compliance committee that regularly report compliance information directly to the sponsor's CEO or the sponsor's senior-most leadership.[14] Together, the compliance officer and compliance committee are accountable for implementing "measures that prevent, detect, and correct fraud, waste, and abuse" as well as ensuring compliance with CMS program requirements.

The requirements for a sponsor's compliance officer, compliance committee, and high-level oversight are summarized below (and described in detail in the Compliance Program Guidelines, Section 50.2.):

- **Compliance officer**: As required by the Compliance Program Guidelines, your compliance officer is a full-time, independent member of senior management responsible for implementing your organization's Medicare compliance program. The Compliance Program Guidelines also state that your compliance officer should not serve in both compliance and an operational area (which would lead to self-policing of the operational area and a conflict of interest). The Compliance Program Guidelines note, however, that your compliance officer can be the same individual as your corporate compliance officer, but CMS strongly recommends that the two positions be staffed independently. Your compliance officer must be an employee of your Part C or Part D organization, parent organization, or corporate affiliate and cannot be an employee of one of your FDRs.[15]
- **Compliance committee**: You must designate a compliance committee to advise your compliance officer and periodically report directly to your governing body on the activities and status of your Medicare compliance program. The compliance

Compliance Officer Independence

Because your compliance officer must be free to raise compliance issues without fear of retaliation, it is a best practice to require your governing body's approval before your compliance officer can be terminated from employment.

[14] 42 CFR §§ 422.503(b)(4)(vi)(B) and 423.504(b)(4)(vi)(B)

[15] 42 CFR §§ 422.503(b)(4)(vi)(B)(1) and 423.504(b)(4)(vi)(B)(1)

committee is accountable to, and must provide regular compliance reports to, the sponsor's senior-most leader and governing body.[16]

The Compliance Program Guidelines state that you need not have a separate Medicare compliance committee as long as the committee addresses Medicare compliance issues. While compliance committee membership varies per the size and scope of sponsors, their membership typically includes the chief financial officer, the chief operating officer, and other senior management, as well as auditors, pharmacists, registered nurses, and nationally certified pharmacy technicians. Other committee membership might include personnel experienced in legal issues, statistical analysts, and staff or managers from various departments within your organization who understand the vulnerabilities within their respective areas of expertise. A sponsor's compliance officer typically chairs the compliance committee, and the chairperson typically reports on the status of the Medicare compliance program to the sponsor's governing body.

- **Governing body and high-level oversight**: Federal regulations[17] also require your governing body to be knowledgeable about corrective actions and exercise reasonable oversight with respect to their implementation and effectiveness. Reasonable oversight, as defined in the Compliance Program Guidelines, includes, but is not limited to, approving the standards of conduct; understanding the compliance program structure; remaining informed about the compliance program outcomes (including the results of internal and external audits); remaining informed about governmental compliance enforcement activity; receiving regularly scheduled, periodic updates from the compliance officer and compliance committee; and reviewing the results of compliance program performance and effectiveness assessments.

Per the Compliance Program Guidelines, your governing body may delegate this oversight to one of its specific committees (e.g., Audit Committee of the Board of Directors or Compliance Committee of the Board of Directors), but your governing body as a whole remains accountable for reviewing the status of your Medicare compliance program, including corrective actions. The scope of the delegation from the full governing body to the governing body committee also must be clear in the committee's charter and reporting.

Effective lines of communication between your compliance officer and compliance committee and your employees, managers, governing body members, enrollees, and FDRs is a core compliance plan requirement, per federal regulations.[18] This requirement and effective approaches for establishing effective lines of communication are discussed further in Section 4.2.2.

3.2.2. Special Investigation Unit

An SIU is an internal investigative unit responsible for FWA investigations, including fraud detection (see Sections 3.1.2. and 5), preliminary investigation (see Sections 3.1.4. and 7), and referral activities (see Sections 3.1.5. and 8), at both the sponsor and FDR levels. The SIU is often a separate unit from the

[16] 42 CFR §§ 422.503(b)(4)(vi)(B) and 423.504(b)(4)(vi)(B)

[17] 42 CFR §§ 422.503(b)(4)(vi)(B) and 423.504(b)(4)(vi)(B)

[18] 42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

compliance or internal audit department. Although separate, all units operate in coordination under the control of your sponsor's governing body. Depending on your organization's size and resources, however, SIU functions may be assigned to investigative staff from your compliance department per Compliance Program Guidelines.

While SIU job titles and descriptions vary, most SIUs have personnel fitting in the following three categories:

- A full-time **director or manager** responsible for day-to-day operations management
- **Investigators** responsible for determining whether investigation subjects are, or are not, committing fraud in violation of state or federal law
- **Analysts** with backgrounds in data mining, billing, coding, or research to make recommendations on opening and closing cases

Job Descriptions

When Special Investigation Unit (SIU) job descriptions are developed, the following should be considered:

- Education and certification requirements
- Minimum years of experience
- Requisite related or direct experience
- Mandatory and desired technical skills (e.g., data mining, interviewing, proficiency with certain software)
- Required oral and written communications skills
- Fulfills requirements to regularly update or refresh skills/maintain certifications

Larger SIUs may also include:

- **Hotline analysts** to answer and document all calls to the sponsor's FWA hotline and handle other allegations. A sponsor may choose to designate hotline call answering to either the SIU or the compliance department or both.
- **Physicians and nurses** to analyze the medical necessity aspects of cases.
- **Certified professional coders and billers** to analyze claims for upcoding and other billing schemes.
- **Administrative personnel** to help organize case files and ensure evidence is properly documented, handled, stored, and preserved.

3.2.3. Other Personnel or Teams Involved with Fraud

To address all fraud management life-cycle activities, a compliance officer and the compliance committee often work with a wide variety of sponsor personnel. They also may mainstream anti-fraud functions by creating teams within or across business units.

Such teams may include:

- **Fraud corrective action team(s)** to develop and implement immediate actions and corrective actions to stop fraud, reduce fraud losses, and minimize the effort and expense required to recover or correct the harm of fraudulent activity (see Section 3.1.3.).
- A **fraud aftercare team** tasked with helping enrollees recover from events of fraud and identity theft.
- A **human resources fraud team** to ensure that adherence to standards of conduct and other FWA-related performance measures are included in employees' annual performance reviews and are tied to compensation. This team may also manage employee support programs (to reduce the chance employees in crisis will turn to fraud to make ends meet) and ask departing employees during exit interviews about their knowledge of any existing FWA within the organization, its providers, or enrollees.
- **A credentialing team** to check all employees, providers, governing body members, officers, directors, and FDRs against HHS OIG exclusion lists and General Services Administration (GSA) debarment lists both before hiring or contracting and monthly thereafter.

- A **fraud finance team** to manage collection of restitution and repayment of overpayments.
- A **fraud training team** to provide initial and annual training to employees, providers, governing body members, officers, and directors of FDRs. Training ideally focuses on institutional integrity and federal laws against fraud, as well as evolving risk areas.
- A **fraud outreach team** to communicate to enrollees, employees, providers, downstream vendors, and insurance brokers your organization's commitment to institutional integrity, the sophistication of your organization's fraud prevention and detection activities, the likelihood of fraud perpetrators being caught and punished, and the important role everyone plays in recognizing and reporting fraud.
- An **internal monitoring and audit team** responsible for conducting periodic internal monitoring and auditing based on annual risk assessments.
- A **data mapping team** to identify all possible data elements (e.g., protected health information [PHI] from accounts receivable information flows, consumer market activity, health information

flows, operational flow activity, product market activity, and service market activity) and to set the framework enabling your investigative team to derive intelligence from data.

- A **fraud metrics team** (independent of the compliance officer) to estimate losses from fraud, make informed judgments about the level of investment required to counter it, and create and track metrics on the success of anti-fraud activities. These metrics are tied to better outcomes (e.g., reduced losses to fraud) and not just activity (e.g., the number of investigations, prosecutions).

3.3. Essential Tools

Effective tools are critical to preventing, detecting, and combating fraud. Essential tools for sponsors include:

- **Data analytics** software enabling your investigative team to analyze large data sets and find patterns indicating fraud activity.
- **Measurement and tracking tools**, such as dashboards, scorecards, self-assessment tools, and other mechanisms, to measure FWA compliance within your sponsor's operational areas and the program compliance of your providers, downstream vendors, and insurance brokers.
- **Reporting tools,** such as telephone hotlines, mail drops, or suggestion boxes enable employees and enrollees to report FWA without concern about retribution.

4. PREVENTION

Many payment errors are simply mistakes. The vast majority of healthcare professionals are honest and bill their services appropriately. But a handful of dishonest healthcare professionals are intent on abusing the use of or defrauding Part C and Part D sponsors. The fraud schemes they commit deplete funds that should be spent on treatments and medicines.

Fraud perpetrators could be ready to exploit each part of your daily operations for illicit gain. You need to be aggressive in your daily duties to prevent fraud, not just to detect it. It is far easier to improve systems than to recover dollars already lost to it. The more fraud a sponsor prevents, the lower its payout for fraudulent claims.

This chapter describes how to make your fraud prevention activities conform to federal regulations[19] while integrating:

- Top-down fraud prevention approaches (increasing the difficulty of committing fraud and strengthen the perception that fraud perpetrators will be caught and punished)
- Bottom-up fraud prevention approaches (promoting institutional integrity and a climate where enrollees and employees actively seek out and report fraud)
- Collaboration and information sharing with associations and groups involved in the fight against healthcare fraud

Compliance vs. Prevention and the Fraud Management Life Cycle

Federal regulations* mandate that sponsors "adopt and implement an effective compliance program, which must include measures that prevent, detect, and correct non-compliance with CMS's program requirements as well as **measures that prevent, detect, and correct fraud, waste, and abuse**." By that definition, "compliance" includes the entire fraud management life cycle described in Section 3.1., with prevention being a key component.

Because compliance is much broader than fraud management—and entails obeying the law and regulatory requirements in general—it is important to refer to the Compliance Program Guidelines for detailed guidance on establishing and maintaining an effective overall compliance program.

*42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

[19]42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

Much of this section addresses the Medicare compliance program core elements mandated by federal regulation. However, the text is organized from an outreach and education perspective, not a compliance perspective, to help sponsors design prevention activities that inform, motivate, and achieve results. Please refer to the Compliance Program Guidelines for detailed guidance for establishing and maintaining an effective overall Medicare compliance program. The following table details where Medicare compliance program core elements mandated in the federal regulations are discussed in this publication in terms of fraud only.

Medicare Part C and Part D Compliance Program Core Requirement

Compliance Plan Element	Description
Written standards (see Section 4.1.2.)	Develop written policies, procedures, and standards of conduct articulating how your sponsor prevents, detects, and corrects FWA and its commitment to complying with all applicable federal and state standards.
Compliance officer and compliance committee (see Section 3.2.1.)	Designate a compliance officer and a compliance committee that regularly provides compliance reports directly to the CEO or other senior management and is accountable to sponsor leadership.
Training and education (see Sections 4.1.5., 4.2.1., and 4.2.6.)	Provide effective FWA training and education for your CEO, governing body members, managers, employees, and FDRs when they join your organization and annually thereafter.
Effective lines of communication (see Section 4.2.2.)	Maintain effective lines of communication ensuring confidentiality between your compliance officer, compliance committee members, governing body members, managers, employees, and FDRs. Such lines of communication must be accessible to all and include at least one method of reporting fraud and non-compliance anonymously.
Enforcement of written standards through well-publicized disciplinary standards (see Sections 4.1.2. and 4.1.3.)	Publicize and enforce disciplinary standards for non-compliance with written policies, procedures, and standards of conduct to encourage participation in your Medicare compliance program.
System for routine monitoring and identification of compliance risks (see Section 4.1.4.)	Establish and implement effective routine systems for monitoring and identifying compliance risks.
System to promptly respond to and investigate potential compliance issues (see Sections 3.1.3., 3.1.4., and 3.1.5.)	Develop policies and systems for promptly responding to compliance issues as they are raised, investigating and correcting potential compliance problems to reduce the potential for recurrence, and ensuring ongoing compliance with CMS requirements.
Per 42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)	

4.1. Top-Down Approaches

This chapter divides prevention activities into top-down and bottom-up approaches (see Section 4.2. below) to help sponsors design prevention activities that inform, motivate, and achieve results. When it comes to fraud prevention, the way messages, materials, and activities are framed is critical. Too much of a top-down orientation can make it hard to mobilize your organization's employees as your eyes and ears against fraud. At worst, you could alienate them and make them feel that everyone is under suspicion and being monitored.

Top-down approaches (balanced with the bottom-up approaches) have a dual focus:

- Using standards of conduct; policies and procedures; and routine monitoring, auditing, and risk assessment to increase the difficulty of committing fraud.
- Increasing the perception that fraud perpetrators will be caught and punished

Top-down approaches include:

- Leadership commitment
- Written standards
- Enforcement of standards
- Routine monitoring, auditing, and risk assessment
- Outreach on top-down approaches to increase the perception that fraud perpetrators will be caught and punished

Institutional Integrity Best Practice

An industry best practice is promulgating a resolution of the full governing body stating the sponsor's commitment to compliant, lawful, and ethical conduct. This communicates to employees and FDRs that compliance and ethics are valued and important to those at the highest levels of authority in the company.

Top-down approaches to preventing fraud should be balanced with bottom-up approaches promoting institutional integrity and a climate in which enrollees and employees actively seek out and report fraud.

Each approach is described below.

4.1.1. Leadership Commitment

One of the most important top-down approaches is leadership commitment. Senior management and leaders at all levels define how fraud is seen within your organization. Ideally, leadership frames fraud as a challenge everyone is responsible for identifying and reporting in good faith — taking great care to avoid framing fraud as something that cannot be acknowledged or openly discussed. To accomplish this, management needs to communicate clearly that the following is not tolerated:

- Fraudulent activity and non-compliance with CMS program requirements
- Retaliating against employees who report potential fraud

They also need to communicate:

- Strong and explicit organizational commitment to CMS compliance standards and institutional integrity
- Preventing and reporting fraud is a top priority for everyone — not just a concern for investigative, compliance, or internal audit staff

Ideally, these communications are reinforced regularly. Equally importantly, senior management needs to respond promptly when fraudulent activity is detected to:

- Comply with federal regulations[20]
- Build further confidence that fraud is not tolerated
- Encourage employees to act as your organization's eyes and ears against fraud (see Section 4.2.6.)

4.1.2. Written Standards

A core compliance plan requirement, per federal regulations,[21] is written policies, procedures, and standards of conduct articulating how your sponsor prevents, detects, and corrects FWA, and its commitment to complying with all applicable federal and state standards. Per the Compliance Program Guidelines, you need to have a method to demonstrate that your written standards were distributed to your employees as well as your FDRs' employees. Your written standards need to be sufficiently broad to capture the principles of institutional integrity, yet specific enough to provide practical guidance to employees and others for dealing with potential compliance issues. These standards are to be updated, as necessary, to incorporate any changes in applicable laws, regulations, and other requirements.

Corporate Code of Conduct?

You can use your corporate standards of conduct (also known in some organizations as the "code of conduct" or by other similar names) to comply with the standards of conduct requirement.* You can include your standards of conduct for Part C and Part D in your overall corporate standards of conduct or you may state them in a separate Medicare-specific, stand-alone document, per the Compliance Program Guidelines.

*42 CFR §§ 422.503(b)(4)(vi)(A) and 423.504(b)(4)(vi)(A)

Standards of Conduct. Written standards of conduct that explicitly describe and prohibit fraudulent activity are a powerful tool. They give employees a clear framework for institutional integrity and the understanding that fraud will not be tolerated. They also play an important role in setting your expectations for FDRs. The Compliance Program Guidelines

[20]42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

[21]42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

recommend sharing your standards of conduct with your FDRs or ensuring they have comparable standards of conduct of their own.

To be a powerful force against fraud, standards of conduct:

- **Define institutional commitment**: Per federal regulations,[22] your standards of conduct should state your organization's commitment to complying with all applicable federal and state standards and laws.
- **Define fraudulent activity and explain sanctions**: Per federal regulations,[23] you are required to have disciplinary standards that define fraudulent activity and explain sanctions. Appropriate sanctions, including termination of employment or contractual relationship, are an important deterrent against fraud. An industry best practice is including your disciplinary standards in your standards of conduct so that your standards of conduct clearly provide examples of and forbid fraudulent activity.
- **Obtain explicit commitment**: Per the Compliance Program Guidelines, you must distribute your standards of conduct to new employees within 90 days of hire and annually. You also must distribute them whenever your standards of conduct are updated. An industry best practice is requiring employees to sign a statement confirming they have received and read your standards of conduct and will adhere to them. Getting explicit commitment makes sure that everyone knows what is expected.
- **Require reporting**: Per the Compliance Program Guidelines, requiring in your standards of conduct that employees report suspected fraud (see Section 4.2.2.) makes it clear that reporting fraud is everyone's responsibility.
- **Require employee declarations**: An industry best practice is including in your standards of conduct a requirement that all employees immediately disclose any conflicts of interest (see Section 2.2.5.) or any debarment, exclusion, or other event making them ineligible to perform work related directly or indirectly to federal healthcare programs.
- **Include performance measurement**: Employees need to understand that their performance is measured against the standards of conduct. They also need to know who determines they are adhering to the standards of conduct and how this is done.

Policies and Procedures. Your written policies and procedures represent your response to day-to-day risks of fraudulent activity and the systems you have in place to prevent, detect, and correct fraud. They include:

- **A broad range of policies and procedures that can prevent or lower the risk of fraudulent activity**, although their principal purpose is something else. For example, institutional values, staff training programs, and leadership meetings are not designed specifically to combat fraud.

[22] 42 CFR §§ 422.503(b)(4)(vi)(A)(1) and 423.504(b)(4)(vi)(A)(1)

[23] 42 CFR §§ 422.503(b)(4)(vi)(E) and 423.504(b)(4)(vi)(E)

But if consciously created or tailored with fraud prevention in mind, they can play a key role in preventing and mitigating fraud.

- **Policies and procedures specific to the fraud management life cycle,** as explained in Section 3.1., per federal regulations[24] and the Compliance Program Guidelines dictate that your policies and procedures are to be prepared and updated carefully and include required sections on:
    - Your organizational commitment to complying with all applicable federal and state standards.
    - How you implement your Medicare compliance program, how you promptly respond to misconduct and compliance concerns as they are raised, and how you investigate and resolve compliance problems to reduce the potential for recurrence and ensure compliance with CMS requirements moving forward. These policies and procedures are to cover self-evaluations, internal monitoring, internal and external audits, remedial actions, and reporting to appropriate parties (i.e., the CMS NBI MEDIC or law enforcement). It is also required that FDRs be included in these policies and procedures.
    - How you conduct corrective actions (e.g., your organization's repayment to CMS of overpayments, disciplinary actions against responsible employees) when you discover evidence of misconduct related to payment or delivery of items or services under your Part C or Part D contract.
    - Guidance to employees and others for dealing with potential compliance issues.
    - The methods employees can use to report fraud and compliance issues confidentially and in good faith. It is required at least one method for reporting fraud be anonymous.
    - Guidance to management for how to create a culture of non-intimidation and non-retaliation for good faith reporting of potential fraud or non-compliance.
    - The procedures in place for your compliance officer and compliance committee to report periodically and directly to your governing body about the activities and status of your Medicare compliance program, including issues identified, investigated, and resolved by the Medicare compliance program.
    - The procedures in place to ensure your governing body is knowledgeable about the content and operation of your Medicare compliance program and exercises reasonable oversight over its implementation and effectiveness.
    - The system you have in place to ensure your employees, CEO, governing body members, Part C or Part D senior administrator, managers, and FDRs receive compliance training as part of their orientation and annually thereafter.

Fraud is only a narrow focus of policies and procedures documents. The discussion above is limited to fraud. An effective Medicare compliance program needs many other policies and procedures.

[24] 42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

4.1.3. Enforcement of Standards

Another core compliance plan requirement is enforcement of written standards through well-publicized disciplinary standards.[25] An industry best practice, as noted in Section 4.1.2., is including your disciplinary standards in your standards of conduct. The proportionate sanctions in your disciplinary standards can include oral or written warnings, performance improvement plans, mandatory retraining, suspension, transfer, termination of employment or contractual relationship, and prosecution.

Importance of Disciplinary Standards

Well-publicized disciplinary standards are mandated per federal regulations.* Your disciplinary standards must be clearly tied to violations of your standards of conduct. When sanctions are not clearly spelled out, employees and FDRs can claim innocence through lack of awareness when accused of violations. When sanctions are clearly spelled out, there are no excuses.

*42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

When disciplinary standards make clear that violations of written standards may result in appropriate disciplinary action, they send a clear message that fraudulent activity will not be tolerated. They may also deter employees and FDRs from considering fraudulent activity — but only if the disciplinary standards are applied consistently and there is a strong likelihood fraudulent activity will be detected. For this reason, it is critical to take action on fraud no matter where it is found in your organization — both to comply with federal regulations[26] and to send a strong message about your commitment to institutional integrity.

Per the Compliance Program Guidelines, you should periodically review disciplinary records to ensure that disciplinary actions are appropriate to the gravity of the violation, fairly and consistently administered, and imposed within a reasonable time frame. The Compliance Program Guidelines also recommend including appropriate contract provisions in FDR contracts to ensure enforcement of your and their standards of conduct.

Publicizing disciplinary standards is discussed in Section 4.1.5.

4.1.4. Routine Monitoring, Auditing, and Risk Assessment

A proactive system for routine monitoring and identification of FWA compliance risks is another core compliance plan requirement.[27] You are required to include FDRs (whether they are located in the United States or offshore) in your system for routine monitoring and identification of FWA compliance risks. Your compliance officer and compliance committee (see Section 3.2.1.) are responsible for oversight and are required to report directly to your governing body on issues identified, investigated, and resolved.[28]

[25]42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

[26]42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

[27]42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

[28]42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

The purpose of routine monitoring, auditing, and risk assessment is to:

- Evaluate compliance with Part C and Part D benefit regulations, sub-regulatory guidance, contractual agreements, all applicable federal and state standards, and your policies and procedures
- Rapidly detect potential issues, problems, or violations for corrective action (see Section 3.1.3.), initial investigation (see Section 3.1.4.), and possibly referral (see Section 3.1.5.)

Performance Indicator Definitions

The definitions for performance indicators are, ideally, detailed enough to ensure that different people at different times, given the task of collecting data for a given indicator, will collect identical types of data.

A proactive system for routine monitoring and identification of FWA compliance risks includes the following six elements:

- **Risk assessments at least annually**: An effective monitoring and auditing program begins with a formal baseline assessment of your major compliance and FWA risks, at least annually. Each business unit and FDR is assessed for the types and levels of risks they present to all Medicare business operational areas. Identified risks are then ranked to determine which ones could have the greatest effect on Part C and Part D programs and used to prioritize your monitoring and auditing work plan accordingly.

Risk Assessment Best Practice

An industry best practice is reviewing FDRs' compliance policies and procedures and standards of conduct as part of annual risk assessments to identify FDRs for periodic monitoring.

- **Monitoring based on risk assessments**: Monitoring is routine quality control and measurement of business unit performance to ensure processes are working even when no specific problems have been identified. Such monitoring helps to ensure corrective actions are undertaken and identified risks are mitigated. Monitoring activities typically involve measuring compliance against precisely defined performance indicators tied to specific objectives. Measuring your employees' perceptions of your sponsor's commitment to fighting fraud and gauging change over time can also be part of this process. Monitoring research can include spot checks, focus groups, group interviews, confidential interviews, structured questionnaires, direct observations, and unannounced site visits.
- **Internal and external auditing based on risk assessments**: Audits are a formal review of a sponsor's past compliance, with a particular set of internal (e.g., policies and procedures) or external (e.g., laws and regulations) standards used as base measures. The scope of internal auditing may be broad. Besides evaluating compliance with Part C and Part D benefit regulations, sub-regulatory guidance, contractual agreements, all applicable federal and state standards, and your policies and procedures, internal auditing may also include such topics as the productivity of operations, reliability of financial reporting, and safeguarding of assets. Your audit system should

include audits by external auditors, as appropriate.[29] Using independent external auditors to audit your records and perform a gap analysis against CMS requirements is an industry best practice for ensuring you can demonstrate compliance to CMS auditors.

Prevention Best Practice

Tying a business unit's monitoring and auditing results to its leaders' compensation is a best practice.

- **Monitoring and auditing work plan**: The Compliance Program Guidelines at Section 50.6.1 requires that the compliance officer, in consultation with the compliance committee develop a monitoring and auditing work plan addressing the risks associated with Part C and Part D programs. The audit plan is to be reviewed and revised throughout the year as new indicators for focused audits emerge. The audit plan details the number of internal audits to be performed; audit schedules, including start and end dates; whether the audits will be announced or unannounced; whether the audits will be desk audits or on site; the audit methodology; necessary resources; persons responsible; final audit report due dates, including findings and recommendations; and follow-up activities from findings and recommendations.[30] The Compliance Program Guidelines state that work plans must detail how FDRs will be identified for auditing and recommends conducting a number of on-site FDR audits as a best practice.
- **Measurement tools**: An industry best practice is developing enterprise-wide metric reports and measurement tools (e.g., dashboards, scorecards, self-assessments). They can be powerful tools to help you visualize and relate different views of data and evaluate operational compliance and Medicare compliance program effectiveness.
- **Follow-up and corrective action**: You are required to adequately address any monitoring or auditing result indicative of potential FWA or non-compliance (see Sections 3.1.3. and 6).[31] In cases of potential fraud, a decision to refer a case to the CMS NBI MEDIC needs to be made promptly after the presence of or a reasonable suspicion of fraudulent activity has been detected (see Sections 3.1.5. and 8). If you do not have the time or resources to investigate the potential fraud or abuse in a timely manner, you are to turn the investigation over to the CMS NBI MEDIC within 30 days, per the Compliance Program Guidelines at Section 50.7.1.

[29] 42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

[30] 42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

[31] 42 CFR § 422.503(b)(4)(vi)

4.1.5. Outreach on Top-Down Approaches

Training and education is another core compliance plan requirement.[32] It is an industry best practice for training and education initiatives to address both top-down and bottom-up approaches to preventing fraud:

- Information about the sophistication of your organization's fraud prevention and detection activities and the likelihood of fraud perpetrators being caught and punished reflects a top-down approach.
- Information about your organization's commitment to institutional integrity and the important role everyone plays in recognizing and reporting fraud reflects a bottom-up approach (see Section 4.2.6.).

Disseminating information on top-down approaches is an effective deterrent to fraud. People who may be tempted to commit fraud may not carry through with that act if they know that your sponsor uses routine monitoring, auditing, and risk assessment, and that proportionate sanctions are in place (including termination of employment or contractual relationship) for violations of written standards. These approaches do little good in preventing fraud, however, if potential fraud perpetrators do not know about them and perceive little chance of detection.

To disseminate information about your disciplinary standards and compliance plan to your employees, the Compliance Program Guidelines recommend:

- Newsletters to explain compliance issues and methods
- Discussion about compliance as a regular topic at department staff meetings, in communications with subcontractors, and in the annual general compliance training
- Relevant postings on your Intranet site
- Posters, cafeteria table tents, and other vehicles to emphasize prominently the importance of compliance

For your FDRs, the Compliance Program Guidelines, recommend distributing your written standards (see Section 4.1.2.) to FDR employees through provider guides, business associate agreements, or participation manuals.

Figure 2 shows how to balance information on top-down and bottom-up approaches according to audience category — employees actively looking for and reporting fraud, the uncommitted, and fraud perpetrators — with the goal of moving audience segments toward integrity and active participation in fraud-fighting efforts. This balancing strategy involves:

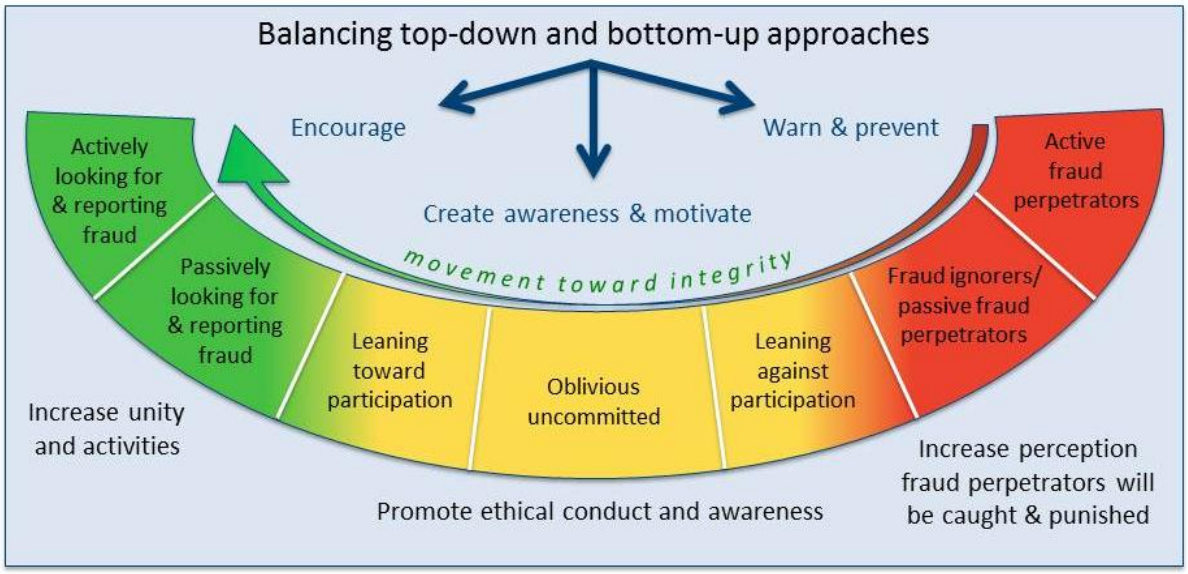
- Increasing unity and activity of employees looking for and reporting fraud (includes but is not limited to investigative staff, compliance staff, and internal audit
- Promoting ethical conduct to motivate the uncommitted

[32] 42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

- Increasing the perception that fraud perpetrators will be caught and punished

It is important to remember to include strategies and messages relevant to all potential audience categories in all of your outreach efforts.

Figure 2: Balancing Anti-Fraud Information by Audience Category



4.2. Bottom-Up Approaches

Some fraud prevention efforts largely focus on top-down approaches. The underlying assumption is that once written standards and robust monitoring and internal control systems are in place, fraudulent activity will be perceived as too risky, causing it to lessen or stop. All too often, however, fraud perpetrators rather than being deterred just become motivated to find ways to reverse engineer fraud prevention and detection systems to exploit vulnerabilities. They simply have too big a stake in preserving their illicit incomes. The solution is balancing top-down approaches with bottom-up ones based on institutional and individual integrity. Creating a culture of institutional integrity and a climate where enrollees and employees actively seek out and report fraud can prevent and detect much more fraud than top-down approaches can alone.

Bottom-up approaches include:

- Compliance training
- Effective lines of communication
- Employee assistance
- Performance reviews
- Regular review of exclusion and debarment lists
- Outreach on bottom-up approaches

Training Best Practice

The best FWA training approach is to engage employees in substantive discussions reinforcing your compliance with applicable laws, regulations, standards, and principles.

Each of these approaches is described below.

4.2.1. Compliance Training

Compliance training is a required part of Medicare compliance programs per federal regulations.[33] These regulations mandate your sponsors provide effective FWA training and education to your CEO, governing body members, managers, employees, and FDRs when they join your organization and annually thereafter. Your compliance training "must ensure that employees are aware of the Medicare requirements related to their job function," per the Compliance Program Guidelines.

Potential Perception Pitfall

Do not let your employees think a zero-tolerance policy against fraud means it is not acceptable to admit it takes place. Make it culturally safe to talk about the high risk of fraud in healthcare and emphasize you want everyone to talk about fraud as part of your organizational commitment to reduce and prevent it.

The Compliance Program Guidelines, along with a May 8, 2012, Health Plan Management System (HPMS) memo, also recommend you retain adequate records of your training of employees, managers, and governing body members, including attendance logs, certificates of completion, electronic certifications, employee attestations, and material distributed at training sessions. The memo also recommends contracts with FDRs require them to maintain compliance training records as follows:

- Keep all training documentation at each individual entity's site (e.g., the lowest level entity would keep its documentation; the next highest level entity would keep its documentation).
- The lowest level entity completes an attestation and sends it to the next higher level entity. For example, if a pharmacy chain has multiple retail stores, each retail store would keep the logs and certificates, and would send the attestation to the regional or corporate office.
- Attestations are "rolled" up until there is one attestation for each FDR. For example, if a pharmacy chain has numerous retail stores and has regional offices, each regional office would collect the attestations from the retail stores in its particular area. The regional office would send the corporate office one regional attestation. The corporate office would then send the Part C or Part D sponsor one attestation for the entire company.

You and your FDRs are required to retain compliance training documents for 10 years and must provide them to CMS upon request.[34]

General Compliance Training. It is very important to educate and mobilize employees and FDRs in the effort to identify and report fraud. Sometimes when they suspect fraud, they may opt not to report it because they are afraid of retaliation or think nothing will be done. Also, if your training is too top-down

[33] 42 CFR §§ 422.503(b)(4)(vi)(C) and 423.504(b)(4)(vi)(C)

[34] 42 CFR §§ 422.504(e) and 423.505(e)

oriented, they may feel alienated by being made to feel that everyone is under suspicion and being monitored.

For general compliance training to effectively mobilize your employees as your organization's eyes and ears, it needs to do more than detail your written standards, disciplinary standards, applicable federal and state standards, and common fraud schemes. These are all critical, but it is also important to build institutional support for protecting and encouraging those who identify and report fraud (see Figure 2). Above all, fraud training needs to be positive, not accusatory, and emphasize that illegal conduct, in any form, eventually harms everybody associated with your sponsor — through lower profits, bad publicity, decreased morale, lower productivity, and possibly poor patient care.

Per the Compliance Program Guidelines, the sponsor's employees (including temporary workers and volunteers) and governing body members, must, at a minimum, receive general compliance training within 90 days of initial hiring, and annually thereafter.

Sponsors must ensure that general compliance information is communicated to their FDRs. The sponsor's compliance expectations can be communicated through distribution of their standards of conduct and/or compliance policies and procedures to FDRs' employees. Distribution may be accomplished through provider guides, business associate agreements, or participation manuals.

Free Web-Based Training Module

CMS has developed a web-based training module that you can use to satisfy your fraud, waste, and abuse training and education requirements. Use of the module is optional. It is available for download in ZIP format at cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Fraud-Waste_Abuse-Training_12_13_11.zip.

The following are examples of topics that the Compliance Program Guidelines recommend for your general compliance training program:

- **A description of your Medicare compliance program**, including a review of compliance policies and procedures, the standards of conduct, and the sponsor's commitment to business ethics and compliance with all Medicare program requirements.
- **An overview of how to ask compliance questions**, request compliance clarification, or report suspected or detected non-compliance. Training should emphasize confidentiality, anonymity, and non-retaliation for compliance-related questions or reports of suspected or detected non-compliance or potential FWA.
- The **requirement** to report to your organization actual or suspected Medicare non-compliance or potential FWA.
- **Examples of non-compliance or FWA** that an employee might observe.
- **A review of the disciplinary guidelines** for non-compliant or fraudulent behavior. The guidelines will 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 compliance and FWA training programs** as a condition of continued employment and a criterion to be included in employee evaluations.
- **A review of policies** related to contracting with the government, such as the laws addressing gifts and gratuities for government employees.
- **A review of potential conflicts of interest** and the sponsor's system for disclosure of conflicts of interest.
- **An overview of HIPAA/Health Information Technology for Economic and Clinical Health**, the CMS Data Use Agreement (if applicable), and the importance of maintaining the confidentiality of personal health information.
- **An overview of the monitoring and auditing process**.
- **A review of the laws that govern employee conduct** in the Medicare program.

See Appendix B of the Compliance Program Guidelines for other examples of laws and regulations that may be discussed in training.

Specialized FWA Training. Per the Compliance Program Guidelines, the sponsor's employees (including temporary workers and volunteers), and governing body members, as well as the FDRs' employees who have involvement in the administration or delivery of Part C and Part D benefits must, at a minimum, receive FWA training within 90 days of initial hiring (or contracting in the case of FDRs), and annually thereafter. Additional, specialized or refresher training may be provided on issues posing FWA risks based on the individual's job function (e.g., pharmacist, statistician, customer service). Training may be provided:

- Upon appointment to a new job function
- When requirements change
- When employees are found to be non-compliant
- As a corrective action to address a non-compliance issue
- When an employee works in an area implicated in past FWA incidents

Sponsors may choose to tailor the training in response to circumstances surrounding potential FWA and specific functions performed by FDRs.

Sponsors must be able to demonstrate that their employees and FDRs have fulfilled these training requirements as applicable. Proof of training may include copies of sign-in sheets, employee attestations, and electronic certifications from the employees taking and completing the training.

Sponsors must provide the FWA training directly to their FDRs or provide appropriate FWA training materials to their FDRs.

The following are examples of topics that the Compliance Program Guidelines recommend you include in your specialized FWA training:

- Laws and regulations related to Part C and Part D FWA (see Section 2.2.)
- Obligations of FDRs to have appropriate policies and procedures to address FWA
- Processes for your organization's employees and FDR employees to report suspected FWA to your organization (or, as to FDR employees, either to your organization directly or to their employers who then must report it to your organization)
- Protection for your employees and your FDR employees who report suspected FWA
- Types of FWA that can occur in work settings

4.2.2. Effective Lines of Communication

Effective lines of communication between your compliance officer and compliance committee (see Section 3.2.1.) and your employees, managers, governing body members, enrollees, and FDRs is another core compliance plan requirement.[35]

Reporting. Regulatory-mandated, effective lines of communication include systems for receiving, recording, and responding to compliance questions or reports of potential FWAs that meet the following criteria:

Mandatory Fraud Reporting

An industry best practice is requiring in your standards of conduct that employees report suspected fraud.

- Maintain confidentiality
- Include at least one way to maintain anonymity (for enrollees uncomfortable reporting potential fraud directly to their providers or employees uncomfortable reporting potential fraud directly to their supervisor or the compliance officer)
- Promote a policy of non-intimidation and non-retaliation for good faith reporting
- Are available to all

The Compliance Program Guidelines require that sponsors make reporting mechanisms user friendly; easy to access and navigate; and available 24 hours a day for employees, members of the governing body, and FDRs. The Compliance Program Guidelines specifically recommend telephone hotlines and mail drops and recommend such as industry best practices:

- Establishing more than one type of reporting mechanism to account for the different ways people communicate or feel comfortable communicating
- Providing the complainant with information regarding expectations of a timely response, confidentiality, non-retaliation, and progress reports when a suspected compliance issue is reported

Another industry best practice is disseminating information about your reporting tools, using both top-down and bottom-up messages (see Figure 2 and Sections 4.1.5. and 4.2.6.). You can use routine reminders, posters, and quizzes during compliance training to help employees and FDRs remember that reporting tools exist. To remind members, you can use flyers, letters, or pamphlets included in their explanation of benefit mailings.

Reporting Response. Prompt preliminary investigation (see Sections 3.1.4. and 7) and corrective action (see Sections 3.1.3. and 6) procedures need to be developed when the presence or a reasonable suspicion of fraudulent activity has been reported. Per the Compliance Program Guidelines, you must begin a

[35] 42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

reasonable inquiry no later than two weeks after the date you identify potential non-compliance or potential FWA.

4.2.3. Employee Assistance

Employees can cross the line between honest and fraudulent behavior when they are under pressure due to financial hardship, family problems, or a desire for lifestyle improvements they cannot afford. Managers and employees need to be trained to observe signs of pressure among their employees and colleagues.

To lower the risk of employees committing fraud when they are under pressure, your organization can take steps to assist employees who might be experiencing challenges.

Drugs Prescribed or Provided by Excluded Providers

Sponsors are prohibited from paying for drugs prescribed or provided by an excluded provider as identified by either the Health and Human Services Office of Inspector General or the General Services Administration, per 42 C.F.R. § 1001.1901. If you discover any claims submitted for drugs prescribed or provided by an excluded provider, investigate immediately, and report the claim to the CMS National Benefit Integrity Medicare Drug Integrity Contractor.

- **Open door policies**: If employees can speak freely, many managers will understand the pressures they are under and work with the employees to help reduce or eliminate these pressures.
- **Employee support programs**: Your organization can offer employees support programs, including treatment for drug and alcohol addiction and counseling for gambling, marital problems, and financial difficulties.
- **Helplines**: Your organization can offer an anonymous helpline so employees can ask for advice about making ethical decisions (and help prevent them from rationalizing unethical behavior).

4.2.4. Performance Reviews

Per the Compliance Program Guidelines, you may consider including compliance as a measure in employees' annual performance reviews. Also, a Health Plan Management System (HPMS) memo dated January 20, 2012, titled "2011 Program Audit Findings and Best Practices," recommended: "Business function leaders should be held accountable for compliance results (i.e., this should influence performance evaluations and incentives)."

4.2.5. Regular Review of Exclusion and Debarment Lists

A lack of staff vetting and security screening can be the root cause of fraud problems. Recruitment checks and controls are the first line of defense in preventing people with criminal backgrounds or past financial difficulty from being affiliated with your sponsor. Per the Compliance Program Guidelines, you are to check all employees, providers, governing body members, officers, directors, and FDRs for eligibility to participate in federal healthcare programs before hiring or contracting, and monthly thereafter. Check them against the HHS OIG exclusion lists at http://exclusions.oig.hhs.gov/ and find out how to sign up to view the GSA exclusions lists at sam.gov/sam/transcript/Quick_Guide_for_Exclusions_v1.7.pdf.

4.2.6. Outreach on Bottom-Up Approaches

As detailed in Section 4.1.5, training and education are core compliance plan requirements. Industry best practice is ensuring that training and education include both top-down and bottom-up approaches to preventing fraud:

- Information about the sophistication of your organization's fraud prevention and detection activities and the likelihood of fraud perpetrators being caught and punished reflects a top-down approach
- Information about your organization's commitment to institutional integrity and the important role everyone plays in recognizing and reporting fraud reflects a bottom-up approach

Bottom-up approaches are critical to promoting institutional integrity and a climate where enrollees and employees actively seek out and report possible fraud. Employees need to understand that preventing fraud is everybody's responsibility — not just a concern for your investigative, compliance, or internal audit staff — and the important role they play as your organization's eyes and ears. As discussed in Section 4.1.1., leadership commitment plays a key role in setting the tone. So does ensuring that information disseminated targets each audience category shown in Figure 2.

To motivate employees who are uncommitted to seeking out and reporting possible fraud, per Figure 2, information disseminated needs to explain how fraud and your organization's fraud-prevention efforts affect them personally:

- How fraud ultimately harms everybody associated with your sponsor — through lower profits, bad publicity, decreased morale, lower productivity, and possibly poor healthcare
- How fraud threatens the integrity and solvency of Medicare and other federal healthcare programs
- How combating fraud is essential to maintaining a healthcare system that is affordable for everyone
- How seriously your sponsor takes institutional integrity and its efforts to prevent, detect, and reduce fraud

Motivating Enrollees

To motivate enrollees and their caretakers to use your fraud-reporting mechanisms, outreach materials need to personalize the cost of fraud at an individual and societal level. In other words, enrollees and their caretakers need to understand how reporting potential fraud is in their interest.

Outreach messages also need to explain what fraud indicators to look out for, how to apply your organization's standards of conduct every day on the job, and the reporting tools your organization has in place.

4.3. Collaboration with Other Anti-Fraud Efforts/Associations/Venues

Collaboration among sponsors, associations, and other entities is key to effectively preventing and detecting fraud in healthcare. With the passage of the Affordable Care Act of 2010, CMS has been given

more resources and statutory authority to prevent and detect fraud in the Medicare program. Many associations and groups have been established to assist people who fight fraud to share information and collaborate to strengthen their efforts in fighting fraud in the healthcare system. This section covers four topics: the Parts C and D Fraud Work Groups, National Health Care Anti-Fraud Association (NHCAA) and other anti-fraud associations, SMP, SHIP, and other consumer organizations.

4.3.1. Parts C and D Fraud Work Groups

The Parts C and D Fraud Work Groups are composed of representatives from Part C and Part D sponsors and serve as a venue to share information about trends and issues they were seeing in their sponsors. Representatives from sponsors, PBMs, CMS, law enforcement, and CMS Program Integrity Contractors gather to share information and discuss current fraud trends and anti-fraud efforts.

Participation in the Parts C and D Fraud Work Group meetings is limited to the groups above, and is not open to the public. This allows sponsor representatives to share sensitive information in a confidential environment. The work group meetings include presentations, breakout sessions, and networking. Because each sponsor generally only has access to its own data, a fraudulent provider or potential problems might fly under the radar. During the work group meetings, sponsors share information about what they have found, and are able to assess the potential risks both locally and nationally.

Members that attend the work group meetings vary in experience and length of time working with Medicare programs. By allowing participants to work together, the meetings enable new attendees to learn from the experiences of veterans and veterans can view issues with fresh eyes. Work group meetings are intended to be held four times a year in different locations across the country. Future dates and locations are posted on the CMS O&E MEDIC website at http://medic-outreach.rainmakerssolutions.com/. Registered and vetted members of the CMS O&E MEDIC website can also register for the work group meetings on the website.

4.3.2. NHCAA and Other Anti-Fraud Associations

As fraud has been increasingly identified to be a major concern in healthcare programs and as the numbers of fraud investigators and compliance specialists have grown, associations have been established and refocused to share information and best practices about this critical topic. Membership in these associations is voluntary, and these organizations provide training regardless of membership:

- **National Health Care Anti-Fraud Association (NHCAA)** was founded in 1985 by private health insurers, federal and state government officials, and other interested organizations. NHCAA exclusively focuses on fighting healthcare fraud. Members include more than 100 private health insurers, representatives from law enforcement, regulatory agencies, and companies who investigate healthcare fraud in the public and private sector. In 2000, NHCAA created the NHCAA Institute for Health Care Fraud Prevention as a separate educational foundation that provides education and training to private- and public-sector healthcare anti-fraud personnel. The mission of NHCAA is to protect and serve the public interest by increasing awareness and improving the detection, investigation, civil and criminal prosecution, and prevention of healthcare fraud. NHCAA pursues this mission by maintaining strong partnerships and providing learning opportunities through the institute. NHCAA provides opportunities for public and private sector information sharing and serves as a national resource for professionals, government representatives, and law enforcement. Membership information is available at nhcaa.org.

- **Health Care Compliance Association (HCCA)** started out as a Special Interest Group of the Medical Group Management Association in 1996 as a forum for healthcare professionals involved in compliance in all aspects of healthcare. HCCA held its first meeting in September 1997. During this first year, in response from members for more local networking opportunities, HCCA established 10 HCCA Regions based on the Health Care Financing Administration's (HCFA's) 10 regions. HCCA's mission is to champion ethical practice and compliance standards and to provide the necessary resources for ethics and compliance professionals and others who share these principles. The organization works to promote quality Medicare compliance programs in healthcare — their introduction, development, and maintenance, to provide a forum for interaction and information exchange to enable members to provide high-quality Medicare compliance programs and to create high-quality educational opportunities for those involved with compliance in the healthcare industry. HCAA provides educational programs, professional networks, monthly newsletters, compliance weekly news updates, Compliance E-News alerts, Health Care Forum Discussion Groups, Annual National Compliance Institute, regional seminars, and cooperative programs with other national organizations. Membership information is available at hcca-info.org.

- **Association of Certified Fraud Examiners (ACFE)** is the world's largest anti-fraud association. The ACFE certifies fraud examiners in the investigation of fraud as a whole. While the ACFE has not historically focused on healthcare fraud, over the last few years more attention has been given to this part of fraud examination. The mission of the ACFE is to reduce fraud by detection and deterrence. ACFE does this by providing administration of the Certified Fraud Examiner (CFE)

examination. ACFE sets high standards for admission, including continuing professional education, and requires its members to meet strict professional conduct and ethical standards, and provide leadership to inspire public confidence in the integrity, objectivity, and professionalism of CFEs. Membership information is available at acfe.com.

- **International Association of Special Investigation Units (IASIU)** was founded by a group of insurance industry fraud investigators in 1984.This non-profit organization's mission is to promote a coordinated effort within the industry to combat insurance fraud. The IASIU does this by providing education and training, developing awareness of the insurance fraud problem, encouraging professional conduct among insurance investigators, and supporting legislation that acts as a deterrent. Membership information is available at iasiu.org.

4.3.3. SMP, SHIP, and Other Consumer Organizations

Organizations that include Medicare consumers are active in combating fraud:

- **Senior Medicare Patrol (SMP)** programs train Medicare beneficiaries to avoid, detect, and prevent healthcare fraud. The SMP program began in 1995 as a demonstration project and is currently under the jurisdiction of the Administration on Aging. During the demonstration phase, the program returned $23 for every $1 spent looking at the fastest growing areas of Medicare fraud. There are 55 SMP projects (in each state, Guam, Puerto Rico, the Virgin Islands and the District of Columbia, plus the National Hispanic SMP). SMP staff train volunteers to conduct outreach to Medicare consumers in their communities through group presentations, exhibiting at community events, answering calls to the SMP help lines, and one-on-one counseling. The SMP and their volunteers teach Medicare beneficiaries how to protect their personal identity, identify and report errors on their healthcare bills, and to identify deceptive healthcare practices, such as illegal marketing, providing unnecessary or inappropriate services, and charging for services that were never provided. When an issue is identified that cannot be handled at this level, the SMP program will refer the information to the CMS NBI MEDIC. For more information about the SMP program in each state refer to smpresource.org.

- **State Health Insurance Assistance Programs (SHIPs)** are CMS-funded programs that offer one-on-one counseling and assistance to people with Medicare and their families. SHIP projects

are in every state, territory, and the District of Columbia. SHIP counselors, most of whom are volunteers, assist Medicare beneficiaries by providing them impartial information on traditional Medicare and Part C and Part D sponsors. SHIPs provide free counseling and assistance via telephone and face-to-face interactive sessions, public education presentations and programs, and media activities. SHIP counselors also provide counseling at events during open enrollment and special election periods. SHIPs are not funded to look for fraud specifically, but they do receive reports of marketing fraud, problems with sponsors, and problems with physicians or suppliers. If the SHIP counselor assisted the Medicare beneficiary in deciding which sponsor to choose, that beneficiary may call the SHIP counselor to report fraud. In some states, the SHIP and the SMP programs are housed in the same organizational unit. In others, they are separate but may share volunteers. The SHIP counselors may refer fraud to the SMP program but may also report this information to the CMS NBI MEDIC. The SHIP website is shiptalk.org.

- **National Center for Benefits Outreach and Enrollment (NCBOE)**, funded through a cooperative agreement with the National Council on Aging, assists organizations in enrolling seniors and younger adults with disabilities with limited means into the benefits programs for which they are eligible. This program has worked to find individuals who are eligible for benefits such as the low income subsidy program and get them involved. The NCBOE has partnered to start Benefit Enrollment Centers in 20 areas of the country, including some of the high-fraud states. As they are assisting individuals, NCBOE representatives often hear stories and complaints from individuals who are not sure where to report the suspicious behavior. The NCBOE will then assist the Medicare consumer in reporting this information to the correct entity. The NCBOE website is ncoa.org/enhance-economic-security/center-for-benefits/.

4.4. "Are We Doing Enough?" Checklist

This checklist was designed to help sponsors assess if they are doing enough to prevent fraud based on the concepts discussed in Section 4. The checklist can be used by both a sponsor and its FDRs. These concepts are industry best practices only and are not required in the federal regulations or the Compliance Program Guidelines. The checklist is also not meant to be inclusive of every prevention activity possible.

Are We Doing Enough? Checklist		
Top-Down Approaches		
Leadership Signals		
1.	Does leadership make clear that they have a zero-tolerance approach to fraud?	
2.	Does leadership make clear that they have a zero-tolerance approach to retaliation against people who report fraud?	
3.	Does leadership make explicit their strong organizational commitment to compliance standards and ethical corporate behavior?	
4.	Does leadership frame fraud as a challenge everyone is responsible for identifying and reporting in good faith?	
5.	Do senior leadership and middle managers emphasize they want employees to talk about the high risk of fraud in healthcare as part of their commitment to reduce and prevent it?	
6.	Are ethics and institutional integrity issues woven into leadership and staff meetings on a regular basis?	
7.	Has your full governing body promulgated a resolution stating your organization's commitment to compliant, lawful, and ethical conduct?	
8.	Does leadership respond quickly when fraudulent activity is detected?	
Written Standards		
9.	Do standards of conduct clearly define fraud and activities that are fraudulent under CMS regulations; all applicable statutory, regulatory, and other Part C and Part D program requirements; and federal, state, and local FWA laws?	
10.	Do standards of conduct emphasize institutional commitment to fighting fraud?	
11.	Do standards of conduct clearly forbid fraudulent activity?	
12.	Are new employees and newly contracted FDRs involved with Part C and Part D programs required to sign standards of conduct certifying that they have read, understand, and agree to comply with their terms?	
13.	Are employees and FDRs involved with Part C and Part D programs required to review and sign standards of conduct annually and whenever standards of conduct are updated?	
14.	Do standards of conduct clearly define the sanctions for failing to comply with expectations for ethical behavior?	
15.	Do standards of conduct give employees and FDRs the duty to report suspected fraudulent activity?	

Are We Doing Enough? Checklist		
16.	Are there conflict of interest requirements that require all employees, governing body members, or FDRs involved in Part C and Part D programs to disclose immediately any conflicts of interest?	
17.	Do standards of conduct require all employees, governing body members, or FDRs involved in Part C and Part D programs to disclose immediately any debarment, exclusion, or other event making them ineligible to perform work related directly or indirectly to federal healthcare programs?	
18.	Do employees understand that their performance is measured against the standards of conduct?	
19.	Do employees know who monitors adherence to the standards of conduct and how?	
20.	Are there procedures for identifying fraud within the organization's network?	
21.	Are there procedures for mitigating any compliance issues found in the organization's network and preventing future misconduct?	
22.	Are there procedures for retaining all records documenting all corrective actions taken to mitigate FWA activity in the delivery of Part C and Part D programs?	
23.	Are there procedures for retaining all records documenting any follow-up compliance reviews after corrective actions were taken to mitigate FWA activity in the delivery of Part C and Part D programs?	
24.	Is there a process for complying with CMS's ten-year record retention requirement?	
25.	Do policies emphasize confidentiality, anonymity, and non-retaliation for compliance-related questions or reports of potential fraud?	
26.	Are there procedures for conducting initial investigations of potential fraud in a timely manner?	
27.	Are there policies and procedures mandating a decision to refer a case to the CMS NBI MEDIC and/or law enforcement promptly when a preliminary investigation leads you to believe a criminal, civil, or administrative law was violated or within 30 days if you do not have the time or resources to investigate?	
28.	Are there procedures for responding in a timely manner to data requests by CMS, the CMS NBI MEDIC, law enforcement, or their designees?	
29.	Are there policies and procedures for cooperating with any federal audits?	
30.	Are there procedures for ensuring employees and FDRs are marketing in accordance with applicable federal and state standards, including state licensing laws and CMS policy?	
31.	Are there procedures for identifying improper coverage determinations, services, or enrollment at any level within the organization's network and properly reporting and repaying, where applicable, any overpayments resulting from inaccurate enrollment numbers in accordance with CMS policy?	
32.	Are there policies ensuring all employees, providers, governing body members, officers, and directors, as well as FDRs, are checked against HHS OIG exclusion lists and GSA debarment lists before hiring or contracting?	

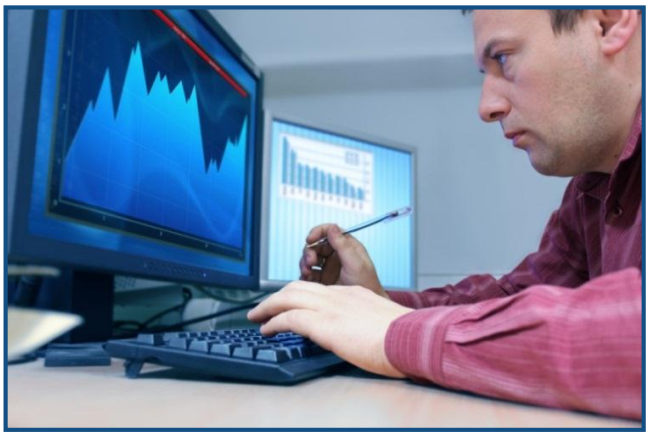
Are We Doing Enough? Checklist		
33.	Are there policies ensuring all employees, providers, governing body members, officers, and directors, as well as FDRs, are checked against HHS OIG exclusion list and GSA debarment list every month?	
34.	Are there procedures for identifying any claims submitted for drugs prescribed by excluded or deceased providers?	
35.	Are there procedures for identifying, reporting, and repaying overpayments made for claims submitted for services or drugs prescribed by excluded or deceased providers?	
36.	Are there procedures for ensuring full disclosure to CMS, upon request, of all pricing decisions for Part D items or services, related data, and pricing records?	
37.	Is there a policy requiring governing body approval before the compliance officer can be terminated from employment?	
38.	Is there a policy mandating the corporate compliance officer and a Medicare compliance officer be staffed separately?	
39.	Is there a policy allowing the compliance officer to meet in executive session with the governing body?	
40.	Do policies and procedures mandate pharmacy & therapeutic (P&T) committee decisions be made in accordance with CMS regulations and guidance?	
41.	Do policies and procedures ensure that all CMS reporting requirements are satisfied regarding potential conflicts of interest and appropriate lobbying disclosure requirements?	
42.	Is there a clear policy on the recovery of losses incurred to fraud?	
43.	Is fighting fraud woven into policies and procedures that can prevent or mitigate the risk of fraudulent activity?	
Enforcement of Standards		
44.	Are there written disciplinary standards with proportionate sanctions for violations of standards of conduct (e.g., oral or written warnings, performance improvement plans, mandatory retraining, suspension, transfer, civil or criminal prosecution)?	
45.	Are standards of conduct enforced consistently?	
46.	Do contracts with FDRs contain provisions indicating violations of the sponsor's standards of conduct may result in termination of their contractual relationships and referral to law enforcement for prosecution?	
47.	Are records of discipline for compliance violations maintained and regularly reviewed to ensure that disciplinary actions are appropriate to the seriousness of the violation, fairly and consistently administered, and imposed within a reasonable time frame?	
Routine Monitoring, Auditing, and Risk Assessment		
48.	Are risk assessments conducted at least annually?	
49.	Is business unit performance routinely measured against precisely defined performance indicators tied to specific objectives related to combating FWA?	

Are We Doing Enough? Checklist		
50.	Are the definitions of business unit performance indicators related to combating FWA detailed enough to ensure that different people at different times, given the task of collecting data for a given indicator, would collect identical types of data?	
51.	Are internal and external audits regularly conducted?	
52.	Is there an annual auditing and monitoring work plan?	
53.	Does the auditing and monitoring work plan detail how you identify FDRs for periodic monitoring (e.g., reviewing FDRs' compliance policies and procedures and standards of conduct as part of annual risk assessments)?	
54.	Does the auditing and monitoring work plan make it a priority to conduct a certain number of audits of FDRs on site?	
55.	Do fraud investigations lead to revision of policies and systems to remove apparent weaknesses?	
56.	Do compliance issues discovered through monitoring, auditing, and risk assessment lead to revision of policies and systems to remove apparent weaknesses?	
57.	Does the compliance committee or equivalent revise policies and systems on a quarterly basis to remove apparent weaknesses?	
58.	Do contracts with FDRs contain provisions requiring records retention and access rights to these records to CMS or its designee?	
Outreach on Top-Down Approaches		
59.	Is the effectiveness of the organization's fraud detection activities publicized?	
60.	Is the professionalism of the members of your investigative staff and their ability to detect and investigate fraud and work with law enforcement to prosecute it publicized?	
61.	Is the organization's commitment to applying proportionate sanctions to fraud perpetrators, including termination of employment or contractual relationship, publicized?	
62.	Is the organization's commitment to recover losses publicized?	
Bottom-Up Approaches		
Compliance Training		
63.	Do new employees (including volunteers and temporary workers) complete general compliance training within 90 days of hire, and annually thereafter?	
64.	Does general compliance training engage employees in substantive discussions to reinforce their compliance with applicable laws, regulations, standards, and principles?	
65.	Does general compliance training encourage your employees to serve as your organization's eyes and ears against fraud?	

Are We Doing Enough? Checklist		
66.	Do new employees (including temporary workers and volunteers) assigned to Part C and Part D business areas receive specialized FWA training on issues posing compliance risks specific to their job functions (e.g., pharmacist, statistician, claims processors) within 90 days of hire, upon appointment to a new job function, and annually thereafter?	
67.	Do your employees (including temporary workers and volunteers) and governing body members receive specialized FWA training when requirements change?	
68.	Do your employees (including temporary workers and volunteers) and governing body members receive specialized FWA training they are found to be non-compliant, as a corrective action to address a non-compliance issue, or when they work in an area implicated in past FWA?	
69.	Have all those working to counter fraud received specialized professional training and accreditation for their role?	
70.	Do FDR personnel attend the sponsor's compliance training and specialized FWA training or agree to conduct their own Part C and Part D compliance and specialized FWA training?	
Effective Lines of Communication		
71.	Are potential cases of fraud reported promptly to your investigative staff for further investigation?	
72.	Are follow-up investigations stemming from hotline inquiries and other complaints initiated within two weeks of receiving the complaint?	
73.	Are reports of potential fraud made to management kept confidential?	
74.	Is there more than one fraud reporting mechanism (e.g., telephone hotlines, mail drops, suggestion boxes, employee exit interviews, and email)?	
75.	Is there at least one anonymous way to report fraud?	
76.	Are complainants provided with information regarding expectations of a timely response, confidentiality, non-retaliation, and progress reports?	
77.	Are reports about compliance and anti-fraud work a standing governing body agenda item?	
Employee Assistance		
78.	Are employees offered support programs (e.g., treatment for drug and alcohol addiction and counseling for gambling, marital problems, and financial difficulties)?	
79.	Do managers work with employees experiencing difficult times to help them reduce or eliminate pressures?	
80.	Is there an anonymous helpline where employees can ask for advice on making ethical decisions?	
Performance Reviews		
81.	Are business units' monitoring and auditing results tied to their leaders' compensation?	

82.	Are business units' successes in corrective actions related to compliance tied to their leaders' compensation?	
83.	Do employees who meet or exceed standards of conduct expectations receive recognition in their performance reviews?	
84.	Do employees who report fraud confidentially to management receive recognition in their performance reviews?	
85.	Is compliance a measure in employees' performance reviews?	
86.	Do employees who make important contributions to fraud prevention, detection, corrective action, initial investigation, or referral activities receive recognition in their performance reviews?	
87.	Are policies requiring all employees, providers, governing body members, officers, and directors, as well as FDRs, to be checked against HHS OIG exclusion lists and GSA debarment lists before hiring or contracting strictly followed?	
88.	Are policies requiring all employees, provider, governing body members, officers, and directors, as well as FDRs, to be checked against HHS OIG exclusion lists and GSA debarment lists monthly strictly followed?	
89.	Is there a communications plan in place encouraging management to create an anti-fraud culture?	
90.	Is there emphasis on individual and institutional integrity when publicizing the standards of conduct?	
91.	Is the cost of fraud personalized at an individual, organizational, and societal level (e.g., fraud harms everyone associated with the organization through lower profits, bad publicity, decreased morale, lower productivity, and poor care; fraud threatens the integrity and solvency of Medicare and other federal healthcare programs) when communicating to employees about the compliance plan, standards of conduct, and fraud reporting mechanisms?	
92.	Is the cost of fraud personalized at an individual, organizational, and societal level when communicating with FDRs about the sponsor's compliance plan, standards of conduct, and fraud reporting mechanisms?	
93.	Do outreach materials for enrollees publicizing fraud reporting mechanisms personalize the cost of fraud at an individual and societal level?	
94.	Do those working to counter fraud attend Parts C and D Fraud Work Group quarterly meetings?	
95.	Do those working to counter fraud belong to anti-fraud professional associations?	
96.	Do those working to counter fraud collaborate and share information with organizations that help Medicare beneficiaries combat fraud, such as the SMP and SHIP?	

5. DETECTION



Even with the existence of a strong prevention plan, unscrupulous providers, enrollees, and employees may engage in suspect or fraudulent billing and business practices. The purpose of this chapter is to describe detection methods you can implement to enhance your efforts to combat FWA. This chapter provides information on detecting fraud, including sources of data, typical fraud indicators, and methods and resources for data analysis. This overview is followed by specific fraud risks for Part C and Part D. The chapter concludes with a list of additional resources for detecting fraud.

5.1. Overall Detection Considerations

Whether working to detect FWA in Part C or Part D programs, you need to have a familiarity with data sources, data analytics, and resources that support overall detection efforts. This section addresses these topics.

5.1.1. Data Sources and Fraud Indicators

Numerous sources of data or intelligence regarding potential fraud exist, both internal and external to your organization. The following lists of sources are provided as representative examples.

Internal Intelligence Data Sources

- Compliance department/team
- Risk adjustment data (Part C)
- Claims department/team
- Customer service department/team
- Data analysis collaborative team
- Complaint/grievances review team
- Beneficiary enrollment department/team
- Provider credentialing department/team
- Finance department/team

Examples of What to Look for from Internal Data Sources

- ***Provider credentialing department:*** Identify suspect provider applications.
- ***Finance department:*** Spot overpayments and/or voluntary refunds.

External Intelligence Data Sources

- CMS Complaint Tracking Management (CTM) System
- CMS databases (described in Section 5.1.2.)
- CMS NBI MEDIC
- Quarterly Medicare Parts C and D Fraud Work Group meetings
- Media (broadcast, print, digital, social media)

The integration of information from internal and external sources ensures your sponsor has a comprehensive view of the perpetrators and FWA schemes/scams within your service area. Data you gather from these sources can reveal indicators of potential fraud. Examples of useful indicators and ways they are used to detect fraud are described below.

Complaints. Enrollees' complaints (also called grievances) are a concern about the quality of care or other services they are receiving from a provider in a sponsor's network.

Best Practice:
Using Complaints Information

Track complaints data to flag providers and enrollees for further analysis.

Most organizations have online or manual complaint-tracking systems (see Section 5.4.2. for information about developing and using such a system). Indicators to track or trend include the following:

- Complaint receipt date
- Complainant source (enrollee, provider, and other sources)
- Complaint source area (county, ZIP code, area code)
- Provider and provider type included in the allegation
- Type of service and/or item
- Benefit type (inpatient, durable medical equipment prosthetics orthotics and supplies [DMEPOS], home health, drug)
- Number of complaints per provider, enrollee, and benefit type
- Number of complaints that escalated to be treated as Fraud and Abuse grievances (see Fraud and Abuse Grievances, below, for additional information)
- Complaint type categories (billing for services not rendered, solicitation, drug diversion)

Fraud and Abuse Grievances. According to the PDBM, Chapter 18, a "fraud grievance" is a statement, oral or written, alleging that a provider, pharmacy, pharmacist, Medicare Part C sponsor, MA-PD, PBM, Medicare Part D sponsor, or enrollee engaged in the intentional deception or misrepresentation that the individual knows or believes to be false, The individual makes known that the deception could result in an unauthorized benefit to himself or herself or some other person.

The PDBM, Chapter 18, defines an "abuse grievance" as a statement, oral or written, alleging that a provider, pharmacy, pharmacist, Part C sponsor, MA-PD, PBM, Part D sponsor, or enrollee engaged in unethical behavior that the individual should have recognized as such and should have known that such behavior could result in an unauthorized benefit to himself/herself or some other person.

Quick Action Is Important to Fight Fraud

To protect the provider, you may consider withholding provider payment until address, phone, or EFT issues are verified and resolved.

Like complaints, fraud and abuse grievances can be tracked and monitored. You can track outcome and resolution information indicating whether the grievance was referred to another entity for resolution such as the following:

- CMS NBI MEDIC
- Law enforcement
- State medical board
- State licensure board

If the grievance was resolved by your organization's SIU, this information can be categorized by closure types, for example, closed with no additional actions, enrollee misunderstanding, or allegation not substantiated.

Returned Mail/Email and Changed/Non-working Telephone Numbers. Issues such as returned mail or email, or disconnected telephone numbers are potential indicators of a false-front provider or of identity theft. The following provides more details about these indicators:

- Mail returned because of a non-existent correspondence address or because no one at the address knows the recipient
- Email returned because of an invalid email address or closed email account
- Disconnected or out-of-service telephone numbers
- A provider's electronic funds transfer does not successfully complete

CMS Fraud Alerts. CMS issues alerts to sponsors about fraud schemes that law enforcement identifies. Typically, these alerts describe alleged activities involving pharmacies practicing drug diversion or prescribers participating in illegal remuneration schemes. When you receive an alert, you should use the information to add to your fraud monitoring processes and data analytics established to meet program requirements. You also need to:

1. Review your contractual agreements with the identified parties. It would be appropriate for you to consider terminating the contract(s) with the identified parties if law enforcement has issued indictments against particular parties and the terms of your organization's contract(s) authorize contract termination in those circumstances.

2. Take action (including denying or reversing claims) in instances when your own analysis of identified parties' claims activity (prompted by your receipt of a CMS-issued fraud alert) indicates that fraud may be occurring. It is important to note that fraud alerts usually describe alleged fraudulent schemes for which the identified parties have not yet been found legally responsible. For this reason, your decision to deny or reverse claims should be made on a claim-specific basis.

3. Review your past paid claims from entities identified in a fraud alert. With the issuance of a fraud alert, CMS has placed sponsors on notice that they should review claims involving identified providers.[36] To meet the "best knowledge, information, and belief" standard of certification, you should make your best effort to identify claims that may be or may have been part of an alleged fraud scheme and remove them from your prescription drug event (PDE) data submissions.

4. Reverse the affected claims with their pharmacies and reduce their enrollees' true out of pocket (TrOOP) and drug spend amounts accordingly.

Information Gathered at Medicare Parts C and D Fraud Work Group Meetings. The purpose of the Fraud Work Group meetings, usually held on a quarterly basis, is to combat FWA through enhanced collaboration, information sharing, and communication among various stakeholders. These meetings provide a forum to discuss the latest FWA schemes and scams occurring in different service areas, and ways in which sponsors are addressing the perpetrators and their schemes. For more information, please see Section 4.3.1.

Best Practice:
Leveraging Parts C and D Work Group Meetings Intelligence

Following the Medicare Parts C and D Fraud Work Group meeting, compare the identified perpetrators that have been discussed with your data findings and analysis to determine whether the perpetrator or scheme is moving or has moved into your service area.

Repeat Audit Findings. If providers and/or enrollees repeatedly appear in your internal audits or in outside audit reports that consistently include fraud allegations such as billing for services not rendered, upcoding, or drug diversion, consider referring the provider or enrollee to the CMS NBI MEDIC and/or law enforcement for further investigation.

Delinquent Reporting. During claims processing and enrollment, you may determine that additional information is required to verify a service/item or provider enrollment or re-enrollment information. If a provider repeatedly does not respond or refuses to respond to your requests for additional information during the enrollment or claims process, in accordance with his/her provider contract agreement, consider placing the provider on pre-payment review until the provider responds with the requested information and it is verified, as well as referring to the CMS NBI MEDIC and/or law enforcement for further investigation depending on the severity of the issue.

[36] 42 CFR 423.505(k)(3)

Results of National Surveillance Activities During Enrollment Periods. CMS's national surveillance efforts include four oversight activities: Public Event Secret Shopping (secret shopping), Unreported Marketing Events (clipper service review), Surveillance Marketing Allegation Response Team (SMART) activities, and website review. CMS's surveillance activities focus on the following areas:

Best Practice: National Surveillance

Sponsors are increasingly conducting their own surveillance of marketing events to gather information on suspected fraud (as well as non-compliance).

- Public marketing events with agents and/or sponsor representatives
- Scheduled individual appointments with agents and/or sponsor representatives
- Sponsor call centers for information accuracy pertaining to non-renewal plans
- Sponsor marketing materials
- Sponsor websites

CMS's national surveillance program protects beneficiaries from inappropriate marketing by Part C and Part D sponsors.

The surveillance program, overseen by a highly collaborative team of regional and central office managers and staff ("the Surveillance Team"), consists of secret shopping of sponsor marketing events, comprehensive outreach, and collaboration with internal and external partners and other oversight efforts.

Sponsors may use beneficiary enrollment and eligibility data to identify suspect enrollment activity by an agent or broker. For example, if more than 20 beneficiaries enroll on the same day in the same city and/or ZIP code, this situation is an indicator of a suspect enrollment pattern.

Change of Ownership. Change of ownership is of concern when a contracted provider is purchased by another business entity or another Medicare contracted provider and fails to report this change. This situation is often discovered during the validation or re-validation process. Immediate follow up is advisable to determine whether the provider or purchaser is on the HHS OIG List of Excluded Individuals/Entities (LEIE), the Excluded Parties List System (EPLS) found on the System for Award Management website, or has a criminal record.

5.1.2. Data Analytics

The data and data sources listed above provide the basis for analysis to detect the suspicion or actual presence of fraud. Two areas for analysis are especially productive in trying to uncover fraud: scrutiny of beneficiary enrollment data and provider contract information, and surveillance of billing and claims patterns. (Part D-specific data analytics is also detailed in Section 5.3.1.).

When potentially fraudulent or abusive activity is identified, CMS encourages sponsors to refer the matter to the CMS NBI MEDIC. The CMS NBI MEDIC has access to a variety of the CMS data sources listed below. Section 8 explains how to submit referrals to CMS NBI MEDIC. The table below provides a representative list of data sources and tools that can be used by the NBI MEDIC:

Data Sources and Tools for Data Analytics

Data Sources/Tools	Description
Integrated Data Repository (IDR)*	The IDR is a CMS database that houses: ▪ All Medicare claims ▪ Beneficiary and provider enrollment data ▪ All prescription drug event (PDE) data The IDR's purpose is to serve as a centralized and single repository where federal, state, and local agencies can access necessary data.
One Program Integrity (One PI)*	One PI is a portal with two analytical tools that can access and analyze IDR data. Currently, only limited CMS and CMS NBI MEDIC staff can access One PI. There are plans to grant access to more CMS staff and members of law enforcement.
Services Tracking Analysis and Reporting System (STARS)*	The STARS National Database contains data relating to Medicare Part A, Part B, and Part C. STARS can generate leads from Part D data. However, the IDR is the system of record.
Sponsor Claims Data**	Claims data include the following: ▪ Electronic Data Interchange (EDI) data (electronic claims submission file) ▪ Pending claims once they have entered the claims processing system ▪ Finalized claims in the claims processing system
Medicare Beneficiary Enrollment* Database (MBD)	Medicare beneficiary database and enrollment database provided by CMS.
Monthly Full Enrollment File Data (FEFD)**	Monthly enrollment data provided by CMS.
Sponsor Provider Enrollment/ Credentialing Data	Data collected through the provider credentialing and enrollment process by the sponsor.
Coordination of Benefits (COB) Data**	Data provided by the COB contractor that contain other insurance information for Medicare beneficiaries to assist with correct payment.

**CMS NBI MEDIC has access to these data sources.*
***Medicare Part C- and Part D-specific data files*

Data Analysis Focused on Beneficiary Enrollment. For Medicare Part C and Part D, enrollment refers to the processes for signing up Medicare beneficiaries.

To protect beneficiaries from potential identity theft as well as identify risky behavior during the enrollment or re-enrollment process, you need to look for indicators that the submitted information may not be legitimate. The questions below will help you detect suspect enrollment information (These questions were developed from the Program Integrity Manual (PIM), Chapter 4, and industry best practices.):

Questions/Indicators to Consider During Enrollment		
1.	Is the enrollment application complete?	
2.	Is the enrollee located in a designated high-risk area (HRA)?	
3.	Are there original enrollee signatures or only copied signatures? (Consider comparing signatures to previously submitted documents.)	
4.	Is additional information/correspondence being sent through email/mail instead of included with the original application?	
5.	Is someone other than the enrollee calling with additional information?	
6.	Are there markings, revisions, or indications of changes made with correction fluid on the application that are not initialed and dated by the enrollee?	
7.	Is the enrollee's only email address a free email account? (e.g., Hotmail, Gmail)	
8.	If paper information is submitted by the enrollee, does the postmark make sense compared with the enrollee's address?	
9.	Is the enrollee's only telephone number a 1-800 or similar toll-free number?	
10.	Have you received multiple applications for the same enrollee?	
11.	Does information about the enrollee on social network(s) contradict the information provided on the application (e.g., does the enrollee claim a medical degree, but his LinkedIn account shows no evidence of medical school or residency)?	
12.	Is the beneficiary able to easily verify his or her enrollment/sponsor change during the verification call or written response?	
13.	Is documentation of the scope of appointment available?	
14.	How did the individual enroll? (marketing event, individual contact)	

Beneficiary Analysis Examples

Analysis of beneficiary enrollment data can yield valuable results. Examples include:

- Identifying instances of 50 or more sequential enrollee identification numbers that enrolled on the same day with the same agent/broker
- Spotting cases of enrollees with multiple short-term enrollments and comparing them to Schedule II drug data for potential drug diversion activity

Data Analysis Focused on Providers

When contracting with providers, it is important to verify information and clarify any discrepancies found in the submitted documentation (either through telephone interviews or additional document requests). The following information should be verified for all providers:

Data Analysis Strategy: A Key to Success

Sponsors need to develop a data analysis strategy that addresses business objectives, scope of the effort, hardware and software resources, data management principles and tools, staffing, standard analytic methods and routines, and prompt review and reporting of results.

- Excluded Individuals/Entities
- General Services Administration's EPLS
- Current license to practice or conduct business
- Education and training records
- Board certification in each reported specialty area, if required
- Original vs. copied signatures
- DEA number
- Social Security Number
- Employer Identification Number (EIN) or tax identification number
- Accreditation information, if required
- National provider identification number
- Legal business name
- Practice/Business address
- Change of ownership properly reported

The above information can be validated through your organization's background verification system during the contracting or re-contracting process. There are also public sources such as the following that will also assist with verification:

- Yellow Pages: yellowpages.com
- White Pages: whitepages.com
- AnyWho: anywho.com
- 411: 411.com
- Pipl: pipl.com
- Secretary of State searches
- Social networking sites such as LinkedIn

A search of sites such as yellowpages.com or anywho.com allows you to perform reverse address and telephone searches and get information on persons or other businesses that are in the same practice or business space as the enrolling provider.

In addition, when contracting with providers, unsolicited update and/or revision requests may indicate identity theft or suspect providers. The provider may not be aware the request has been submitted. Below is a list of request types that may indicate suspect update/revision requests:

- EIN or tax identification number updates
- Electronic funds transfer (EFT) change requests that include one of the following:
    - Online-only bank
    - Bank is not in the same state as the enrollee
    - Bank is 50 or more miles away from the enrollee's location
    - Bank is out of the country
- Website address has changed, but the original website is still available
- Contact information changes could include:
    - Email address updates to free email accounts
    - Telephone number updates to cell telephone numbers
    - Correspondence address updates that are more than 50 miles from the enrollee's current address or out of state
- Beneficiary left the sponsor but is re-enrolling after a prolonged absence or has enrolled in multiple sponsors over a short period of time
- Electronic/paper remittances redirection to a new vendor or correspondence address

Additional indicators of provider fraud may be detected through data analysis. Below are data analysis examples that focus on suspicious patterns. These types of studies are examples of ways to identify suspect providers that are trying to make their way or have made their way into a sponsor's network:

Provider Analysis Examples

- Identify providers that share a registered agent 100 miles or more outside of your service area.
- Track cases in which providers contact you because they have stopped receiving checks or EFT payments or because their IRS Form 1099 reflects significantly greater income than expected—either of these scenarios may be an indicator of potential identify theft.

(Please see MMCM, Chapter 6, for enrollment requirements. Please see PIM, Chapters 10 and 15, for additional information about suspect enrollment behavior.)

Data Analysis Focused on Billing and Claims. Since fraud is generally committed for financial gain, the analysis of sponsor and provider billing and claims transactions is a fruitful area of pursuit to detect fraud.

As you might expect, access to financial data is key to successful detection efforts. When reviewing immediately available data sources as well as potential new data sources consider the following:

- What data do I have immediately available?
- Are the data formatted and ready for use in data analysis software?
- If not, what level of effort does the data management team need to format the data and make data available?
- How often are the data made available/how often are data produced and updated (daily, monthly, quarterly)?
- How much data do I need to have on hand to develop accurate trends (e.g., two years, three years)?

Data at Work

Medicare Fraud Strike Force operations in eight cities resulted in charges against 91 suspects, including doctors, nurses, and other medical professionals, for alleged participation in a Medicare fraud billing scheme that resulted in an estimated $295 million in false claims. The billing scheme involved home health, physical therapy, mental health services, psychotherapy, and durable medical equipment. Medicare beneficiaries were paid cash to provide information to the providers, who could then submit fraudulent claims to Medicare. The billing scheme was detected, in part, through data analysis.

After you have vetted available data sources and tools, your next step is organizing and implementing your data analysis program. Data analysis comes in multiple forms and levels of complexity. Trend analyses, spike billing reports, identification of overutilization outliers, and predictive modeling are all forms of data analysis.

Data analysis is specific to activity within your service sponsor area and provider and enrollee populations. You may begin with basic analysis such as top-billed enrollee or billing code reports to get a feel for the overall billing for your sponsor. This type of analysis also assists with determining the following:

- Baselines or thresholds for unusual billing trends, utilization outliers, and/or attempts to maximize reimbursement within your service area/sponsor
- High-risk or "hotspot" areas within the service area/sponsor (e.g., specific county or ZIP code with high or spike billing)

Awareness of billing patterns within your sponsor or service area allows you to develop potential FWA algorithms or indicators you may use in data analysis to assess risk for enrollees or providers. These algorithms may predict the likelihood of certain types of providers or enrollees engaging in risky or suspect billing behavior.

Data analysis can range from basic to complex. The table below categorizes types of data analysis based on complexity with examples for each category. These examples can be incorporated into your own data

analysis plan. The sponsor must assess the results of data analysis it conducts to determine which results are applicable to the Medicare program and whether a referral to law enforcement or the CMS NBI MEDIC is warranted. See Section 8 for additional information on referrals.

Types of Data Analysis and Examples

Complexity	Examples
Basic	▪ Identify outlier providers by: ○ Total number of enrollees ○ Total number of services ○ Average number of services per enrollee ○ Average number of prescriptions per enrollee ○ Average total paid per prescription per enrollee ▪ Identify potentially fraudulent agents and brokers by: ○ Total number of enrollees by specific location ○ Total number of enrollees by date and time frame This type of analysis can run on a determined interval such as monthly or quarterly to identify aberrant patterns or anomalies.
Moderate	▪ Develop spike billing reports to detect significant increases in a policy group such as lab services that may indicate a false-front or phantom provider ▪ Develop billing reports to identify significant shifts in billing behavior that may indicate fraud, such as when a physician begins to refer a high percentage of enrollees for drug testing when doing so has not formerly been part of the billing history ▪ Compare DME enrollment and credentialing data to DME competitive bid ZIP codes for potential risky suppliers joining the sponsor, because they can no longer receive payment through original Medicare (Part A and Part B)
Complex	▪ Identify a high utilizing enrollee by the average number of Schedule II drugs purchased per month and compare this information to the enrollee's previous 12 months of prescriptions. Also, compare this information to the prescribing provider's office visits for the enrollee ▪ Compare newly enrolling enrollee location data to agent and broker information for potential fraudulent agents and identify theft

As part of your data strategy, consider, at a minimum, running basic data analysis to ensure you are aware of the types of providers and items/services billed to your sponsor. This awareness will help you identify billing spikes and trends. To be effective, this type of trend analysis needs to be conducted at regular intervals, some daily, and others weekly, monthly, quarterly, or annually. Analysis needs to include consideration of the following questions.

Resource Considerations		
1.	Was there a National Coverage Determination (NCD) revision that led to an increase or decrease?	
2.	Did a new provider group that specializes in an area that increased billing join the sponsor?	
3.	Are there outlier providers, enrollees, or billing codes that need to be flagged for additional review?	
4.	Are there outlier providers and or enrollees that may require further investigation?	

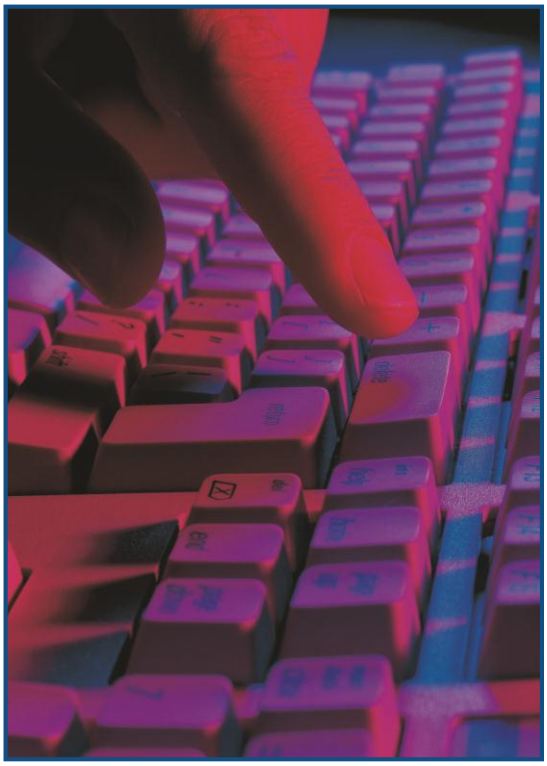
The following are examples of basic data analysis that will assist you with high-level billing views and establish thresholds of aberrant billing for your sponsor:

- Top-billed procedures, items, services, and drugs by benefit type
- Top-billing providers by benefit type, followed by an analysis of categories by benefit type:
    - Specialty type
    - Facility type
    - Billing code ranges
- Top referring/prescribing providers by benefit type
- Top-billed enrollees by benefit type
- Top-billed codes, providers, referring/prescribing providers, and enrollees

Consider performing data analysis at pre-determined intervals specific to certain billing codes, providers, and enrollees. Use the complete results of the data analysis to target areas for monitoring, as well as for gathering additional information from internal and external sources. The benefit of ongoing monitoring is the immediate identification of suspects and risky behavior.

The following are examples of monitoring analysis you can incorporate into your data strategy to identify:

- Top-billing providers and referring/prescribing providers in designated HRAs within your service area
- New providers that have not billed the sponsor in six months since enrolling
- Providers that consistently bill the same submitted amount for the same service/item per enrollee



- Providers that significantly shift their billing (e.g., 50% or greater shift from facet injections to sleep studies or 70% or greater shift from diabetic test strips to back orthotics)
- Enrollees with an overall high claim volume
- Providers that consistently bill more expensive items and services (upcoding)
- Overutilization and underutilization by a provider or multiple providers that consistently bill more or less than policy allows or expects per enrollee (e.g., provider bills 50 boxes of diabetic test strips per enrollee monthly when the policy is three boxes per month)
- Providers that consistently bill same/similar items and/or services for enrollees (e.g., supplier bills a manual wheelchair and power wheelchair at the same time)
- High prescribers by average pills per enrollee
- High-referring providers for DMEPOS
- Providers that are unbundling items/services such as billing individual lab tests that should be billed under one code
- Providers billing more items/services are compared with their peers in the same specialty and service area (peer comparisons)
- Providers billing medically unrelated or unnecessary procedures and services (e.g., diabetic test strips for someone without diabetes)
- Enrollees who purchase drugs at a pharmacy that is 50 miles or more from their home address

As your data analysis program advances, consider enhancing the program by adding more complex data algorithms that include use of cross-claims analysis (to look for duplicate billing or split bills), as well as intelligence gathered from internal and external sources (e.g., policy memoranda, news articles). Below are some trends to look out for that include multiple benefit types and datasets:

- Enrollees in a covered nursing home stay who exclusively receive individual therapy (physical, occupational, speech, and psychotherapy)
- Enrollees with no lab tests and fewer than three physician visits in the last 12 months in his/her billing history but receiving infusion drug therapy
- Enrollees with consecutive approved home health episodes (60-day increments) for one year or more
- Incidents of enrollees who receive a "cocktail" of two or more highly abused drugs within your service area from two or more pharmacies within a 10-day time frame
- Enrollees without a history of psychotropic drug prescriptions six months before entering a community mental health center (CMHC) program who have been in a CMHC or multiple CMHCs for at least one year

Example of Complex Analysis in Pain Management

An analysis of pain management facilities may identify abusive billing and yield multiple suspects for potential investigation. The first step is to look for overprescribed narcotics or other medications without corresponding diagnoses. The second step is to pinpoint potential abusive billing of chiropractic and physical therapy services. The third step is to identify suspect referring providers and durable medical equipment (DME) providers that provide DME to enrollees who may not need it. This will provide a defined group of suspects that may be involved in a pain management scheme.

As your data analysis efforts identify unusual billing patterns or identify suspect individual providers or enrollees, consider monitoring, pre-payment review, or referral to the CMS NBI MEDIC and/or law enforcement for further investigation.

Data analysis also assists with identifying the following:

- Enrollees who received drugs with potential abuse issues or high street value
- Opportunities for front-end claim system editing for overutilization or underutilization of specific items and/or services. (e.g., appearance of stockpiling diabetic test strips for resale)
- Program vulnerabilities/weaknesses within policy and coverage guidelines
- Target areas of educational needs for enrollees and providers

Collaborative review of the results of data analysis can assist you with identifying suspicious patterns. When determining how to review the data analysis results, consider using the data analysis team, as well as staff that are subject matter experts on the relevant policies and medical practice. The review may be through electronic distribution of information or in group meetings—ideally both. The review may enable the following actions:

- Identify suspect providers and enrollees for further investigation
- Pinpoint aberrant or anomalous billing patterns and schemes within your service area
- Determine what reports to run and how often (e.g., daily, weekly, monthly reports/analysis)
- Identify comparison (look-back) time frames (e.g., daily, weekly, monthly, quarterly)
- Establish ongoing monitoring of data analysis reports to ensure quick identification of suspects and schemes
- Implement a data process that helps with ad hoc analysis in response to policy revisions, guideline changes, or hunches.

When data analysis results become available and the collaborative team analyzes this information, establish a process to refer suspects to your SIU, the CMS NBI MEDIC, and other law enforcement. Also, determine how to track referrals, because their outcome will help improve future data analysis planning. Finally, as unusual billing patterns or suspect individual providers/enrollees are identified, consider starting pre-payment review.

Special Circumstance Exceptions

A state may request the Office of the Inspector General (OIG) to make an exception for a provider who has been posted to an OIG exclusion list under special circumstances. For example, if an excluded physician provider holds a position in a state-licensed health center and is the only physician available for the patients, the state may request a special exception from the OIG that the physician's prescriptions written for patients in that health center may be honored and OIG may grant such an exception. The physician would still be excluded from writing prescriptions in other settings such as a hospital or physician practice.

The sponsor would be required to accommodate this exception in its prescription drug event (PDE) systems so the prescription would not be denied.

5.1.3. Resources for Data Analysis

If you have not already integrated the above level of fraud detection into your current enrollment, billing, and claims processes, you may need to conduct a full review of available resources and identify the additional resources that may be required to enhance your fraud-detection program. The following table provides a checklist of essential questions. This information is based on industry best practices.

Resource Considerations		
1.	Do I have full access to data I need to track in order to detect fraud? Are the data valid and current?	
2.	Do I have the necessary hardware and software to verify and track enrollment, billing, and claims information? Does the software need tailoring to track the specific data I need to monitor? Does the software produce standard reports that can be used for fraud detection? Can I write ad hoc reports to obtain special reports containing the data I need?	
3.	Do I have enough qualified staff to perform data management, including the intake of large data sets and publishing these sets to data analysis software? Do they need training on Part C and Part D fraud risks and/or current software and data issues?	

Resource Considerations		
4.	Do I have enough qualified staff to perform data analysis, develop automated data analysis programs, set analytic thresholds, and interpret results? Do they need training on Part C and Part D fraud risks and/or current fraud trends?	
5.	Do I have clinicians, billers, and coders to supplement data analysis?	
6.	Have I developed data analysis algorithms to identify risky behavior and/or providers?	
7.	Do I have standard analysis and reporting processes and procedures to ensure accurate and timely reporting?	
8.	Do I have access to authorities who will take prompt action when fraud is suspected or detected?	
9.	Once suspect enrollees are identified, do I have a process for flagging the provider or enrollee for ongoing monitoring and/or pre-payment review and possible referral to the CMS NBI MEDIC and/or law enforcement?	

5.1.4. Excluded and Deceased Providers

Sponsors are not permitted to make payments to providers excluded by the HHS OIG LEIE and the EPLS found on the System for Award Management website. The sponsors should review these exclusion lists at the time of initial enrollment as well as review monthly updates to the exclusion lists to ensure enrolling or enrolled providers have not been added to those lists. Additionally, they need to have processes in place to prevent payment to excluded providers. If you determine at any time that an excluded provider referred, provided, or prescribed services and/or items, you should report the claims to the CMS NBI MEDIC and/or law enforcement. You can access the exclusion and sanctions file through CMS. The following link will take you to CMS's manual on how to access the Medicare Exclusion Database file that contains HHS OIG and GSA exclusions: cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/mapdhelpdesk/Downloads/MED_UserManual_Final_V10_05202011.pdf.

You should also run current provider enrollment information against the Medicare Master Death Records File (MMDRF) to prevent claims submissions for a deceased provider. If you determine that claims were submitted on behalf of a deceased provider with dates of service after the provider's date of death, you should report the claims to the CMS NBI MEDIC and/or law enforcement. This link will take you to CMS's system of records information on the MMDRF: cms.gov/Regulations-and-Guidance/Guidance/PrivacyActSystemofRecords/Systems-of-Records-Items/CMS1200865.html.

Please see MMCM*, Chapters *6 and 21 and PDBM,* Chapter *9 for excluded provider requirements.

5.2. Part C Specific Risk

One particular Part C risk—excluded and deceased providers and providers lacking credentials—deserves special analysis when you are working to detect fraud (see Section 2.3 for other fraud schemes). This risk involves providers without appropriate credentials.

To ensure the sponsor only contracts with providers that have appropriate credentials and valid licensure, CMS provides guidance detailed in MMCM, Chapter 6, for verifying requirements before contracting. The requirements include the following:

- Medical and business licenses within his/her state and a valid license at the time of enrollment or service date
- Evidence of education and training records to include residency or specialty training, if applicable
- Required board certification in clinical specialty area(s) if the provider indicates he/she is board certified in a specific area

For network providers, determine the following as well:

- A signed contract or participation agreement with the Part C sponsor
- Providers must have signed a participation agreement before they can claim Medicare-covered basic benefits
- Providers are Medicare approved, if required for specific services and items. Approved facilities, including organ transplant facilities, are found here: cms.gov/Regulations-and-Guidance/Legislation/CFCsAndCoPs/index.html
- Providers have the required licenses to operate within their state and are in compliance with all applicable state or federal requirements
- Appropriate accreditation organization has reviewed and approved or certified that the sponsor meets the appropriate standards

If you cannot verify the above information or there are inconsistencies found in the provide contract information, then this is an indicator of suspect provider behavior or potential identification theft. If the provider is unable to provide clarification or validate the information, then refer to the CMS NBI MEDIC and/or law enforcement for further investigation.

(Please see MMCM,* Chapter *6 for provider contracting requirements. Please see PIM*, Chapters *10 and 15, for additional information on suspect provider behavior.)

5.3. Medicare Part D-Specific Risks

Three Part D fraud risks deserve special analytic attention: abnormal patterns in prescribing and dispensing, missing provider identifiers, and a high volume of prescribing to enrollees outside of the expected geographic area. These are summarized below. Also, see Section 2 for other fraud schemes.

5.3.1. Abnormal Patterns of Prescribing or Dispensing

Prescription Drug Event (PDE) Records

Sponsors submit a PDE record to CMS for each prescription filled for their Part D enrollees. Each PDE record contains information about the drug, enrollee, prescriber, and pharmacy. It is critical to use PDE records to identify abnormal patterns of prescribing or dispensing that warrant further scrutiny.

Prescribers. ***The HHS OIG is using PDE records to screen for Part D prescriber outliers and recommended in a June 2013 report that sponsors use data analysis to identify prescribers with questionable patterns as well***. Specifically, the HHS OIG recommended that sponsors compare physicians with similar specialties when conducting such analysis. The following describes how sponsors can replicate the steps the HHS OIG used for its June 2013 report:[37]

1. For each PDE record, identify the prescriber identifier, generally a National Provider Identifier (NPI) number, and match against the National Plan and Provider Enumeration System (NPPES) database to determine which PDE records were prescribed by individuals, as opposed to organizations (e.g., hospitals or group practices).

2. Use the NPPES database to group providers by type, so you can analyze data separately for each category. The NPPES's taxonomy code indicates a provider's specialty and subspecialty, if any. In its data analysis for the June 2013 report, the HHS OIG, for example, grouped all of the nurse practitioners together and all of the dentists together. It also considered general-care physicians to be general practitioners, family practitioners, and internal medicine practitioners with no specialization or a specialization in adults or geriatrics.

3. Eliminate prescribers who are not located in a Core Base Statistical Area (CBSA)—a region around an urban center that has at least 10,000 people—because prescribers in very rural areas may have very different prescribing patterns because of a lack of physicians or specialists in their areas.

4. Use the National Drug Code (NDC) on the PDE record to identify the type of drug and whether it is a brand-name or generic or a Schedule II or III.

5. Use the Health Insurance Claim Number on the PDE record to calculate the total number of enrollees that each prescriber ordered drugs for through your organization during the time period under review.

6. Develop measures to identify prescriber outliers (e.g., above the 75th percentile plus three times the interquartile range) for the time period under review. The HHS OIG used five measures for its June 2013 report:

[37] HHS OIG, Prescribers with Questionable Patters in Medicare Part D (Washington, DC: June 2013). Accessed Aug. 9, 2013, at https://oig.hhs.gov/oei/reports/oei-02-09-00603.pdf.

- Average number of prescriptions per enrollee
- Total number of pharmacies associated with each prescriber
- Percentage of prescriptions that were for Schedule II drugs
- Percentage of prescriptions that were for Schedule III drugs
- Percentage of prescriptions that were for brand-name drugs

When data analysis identifies outliers, they should be referred for education about prescription drug abuse, Part D fraud, and the potential consequences of committing Part D fraud, or for follow-up by the CMS NBI MEDIC and/or law enforcement depending on the extent of their being an outlier.

Pharmacies. The HHS OIG is using PDE records to screen for pharmacies with suspect Part D dispensing patterns and recommended in a May 2012 report that sponsors use data analysis to do the same. The following text describes how sponsors can replicate the steps the HHS OIG used for its May 2012 report.[38] It also suggests some additional measures to use to spot unusual trends and identify suspect pharmacies.

1. To determine which PDE records were billed by retail pharmacies, use the NPI for each pharmacy and match the PDE records to the National Council of Prescription Drug Programs (NCPDP) database. This database contains descriptive information about each pharmacy, including its address, the type of pharmacy (e.g., retail), and ownership status (e.g., XY Retail Chain).
2. Use the NCPDP data to group providers by type, so you can analyze separate data for each type of pharmacy. Retail pharmacies, for example, have different dispensing and billing patterns than do long-term-care pharmacies, mail-order pharmacies, and home infusion pharmacies.
3. Apply the NDC to each PDE record to identify the type of drug prescribed and whether it is a brand name or generic or a Schedule II or III. The HHS OIG used First Databank data for this matching for its May 2012 report.
4. Calculate the total dollar amount and total number of prescriptions billed to Part D per pharmacy type in the time period under review.
5. Calculate the total number of enrollees who received Part D drugs in the time period under review.
6. Calculate the number of different types of drugs billed per pharmacy type in the time period under review. For its May 2012 report, the HHS OIG considered a type of drug to include all drugs with the same name, regardless of dosage or strength.
7. Develop measures to identify pharmacy outliers (e.g., above the 75th percentile plus three times the interquartile range) for the time period under review. The HHS OIG used eight measures for its May 2012 report:
    - Average amount billed per enrollee

[38] HHS OIG, Retail Pharmacies with Questionable Part D Billing (Washington DC, May 2012). Accessed Aug. 8, 2013, at https://oig.hhs.gov/oei/reports/oei-02-09-00600.pdf.

- Average number of prescriptions per enrollee
- Average amount billed per prescriber
- Average number of prescriptions per prescriber
- Percentage of prescriptions that were for Schedule II drugs
- Percentage of prescriptions that were for Schedule III drugs
- Percentage of prescriptions that were for brand-name drugs
- Percentage of prescriptions that were refills

Other suggested measures include:

- Sum total paid
- Percentage of prescriptions that were for enrollees born after Jan. 1, 1963 (or earlier)
- Percentage of prescriptions that were for Schedule II drugs for enrollees born after Jan. 1, 1963 (or earlier)
- Percentage of prescriptions that were for HIV drugs
- Percentage of prescriptions that were for drugs not dispensed as written
- Percentage of prescriptions that were for compound drugs
- Percentage of prescriptions that were for catastrophic coverage

When data analysis identifies outliers, they should be referred for education on prescription drug abuse, Part D fraud, and the potential consequences of committing Part D fraud or for follow up by the CMS NBI MEDIC and/or law enforcement, depending on the extent of their being an outlier.

Drug Utilization Review (DUR)

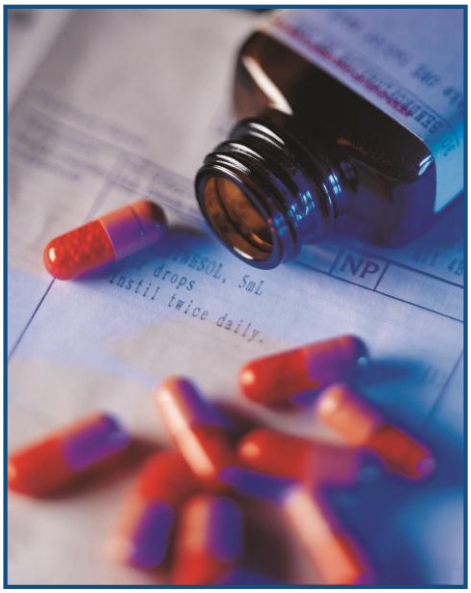
CMS has developed a requirement for sponsors to have in place DUR management systems to prevent erroneous drug claims at the point of sale or distribution, as well as after claims adjudication. DUR systems review claims against current sponsor policies, procedures, and established drug therapy guidelines to ensure that prescribed drug therapies are reviewed both before dispensing the medication and on a retrospective basis. Ideally, DUR detects aberrant patterns that would be identified later through a review of PDE records, but before the actual dispensing of drugs. If anomalies are discovered prior to dispensing, then fraud can be prevented; in addition, fraud can be detected based on patterns identified after claims adjudication and in PDE reviews.

Per the PDBM, Chapter 7, CMS mandates that DUR systems review the following types of elements at the point of sale or the point of distribution:

- Overuse and underuse of prescribed drugs
- Duplicate drug therapy

- Incorrect drug dosage or duration of drug therapy
- Potential drug interactions
- Potential allergy interactions
- Age and gender contraindications

Sponsors are expected to do the following:



- Determine:
    - Classes or types of drugs to review in the DUR
    - DUR edit logic to load
    - DUR edit thresholds
    - DUR revised edit logic and thresholds based on risk assessment
- Compare Medicare Part D claims data with other data sources (if possible) to review the enrollee's medical history to confirm the need for the prescribed medication
- Review Medicare Part D claims data to periodically re-establish appropriate DUR edit baselines or thresholds
- Analyze the Medicare Part D claims to identify new DUR edits

If you identify potentially suspect providers, prescribers, and enrollees during the DUR edit process, they should be referred for education or for follow up by the CMS NBI MEDIC and/or law enforcement, depending on the severity of the situation.

5.3.2. Missing/Invalid Prescriber Identifiers, Especially NPI and DEA Numbers

PDE records allow four types of prescriber identification numbers: **NPIs, DEA numbers, state license numbers,** and **Unique Physician Identification Numbers (UPIN)**. Sponsors are required to certify the accuracy, completeness, and truthfulness of their PDE data. They are also required to ensure that the prescriber identifiers on the PDE records are active and valid, meaning that they are currently assigned to a healthcare provider.[39]

As part of this certification process and to detect fraud, it is critical to screen for missing and invalid NPI and DEA numbers:

Invalid Use of Billing Identifiers

A provider was sentenced to 39 months in prison and three years of supervised release and was ordered to pay $1,045,978 in restitution on two counts of healthcare fraud. The provider purchased a pharmacy that no longer qualified as a pharmacy but continued to submit claims to Medicare Part D. The provider also used the NPI numbers of 16 physicians that stated they did not prescribe the billed drugs.

- **NPI**: Only PDE records containing an active and valid NPI may be submitted to CMS by Part D sponsors. However, having an NPI does not mean that an individual has the authority to prescribe drugs under Part D. Veterinarians, for example, have valid NPIs. For this reason, it is essential to use the information available in the NPPES database to check that the prescriber on the PDE record is a type of prescriber that has the authority to prescribe under state law. The NPPES database contains a taxonomy code indicating a provider's type and specialty, if any, and can be used to avoid paying for drugs ordered by individuals without prescribing authority. When providers apply for an NPI, they are required to certify that the information is correct and they will notify CMS within 30 days of any changes. (Also of note, if a valid NPI cannot be determined at the point of sale and there is no indication of fraud, Part D sponsors are instructed to pay the claim but must acquire a valid NPI before the PDE data may be submitted to CMS.)
- **DEA number**: In the absence of an NPI, you need to consider adding a retrospective authentication data analysis process to ensure that the submitted identifier is correct. This type of analysis also determines whether the prescriber's DEA number is registered to prescribe Schedule II drugs and whether that prescriber is within his or her scope of practice to prescribe Schedule II drugs. By continuously monitoring prescriber identifier data, you can immediately detect potentially aberrant prescribers and providers to include the following:
- Part D drugs inappropriately ordered by individuals who clearly did not have the authority to prescribe, such as veterinarians, massage therapists, athletic trainers, counselors, social workers, and chiropractors. ***The HHS OIG is using PDE data to identify such individuals and recommended sponsors do the same in a June 2013 report.***[40]

[39] CMS, Announcement of Calendar Year (CY) 2012 Medicare Advantage Capitation Rates and Medicare Advantage and Part D Payment Policies and Final Call Letter, April 4, 2011.

[40] HHS OIG, Medicare Inappropriately Paid for Drugs Ordered by Individuals without Prescribing Authority (Washington, DC, June 2013). Accessed Aug. 9, 2013, at https://oig.hhs.gov/oei/reports/oei-02-09-00608.pdf.

- Overpayments because of claims submitted with deceased or excluded prescribers (see Section 5.1.4. for more on this issue)

5.3.3. High Volume of Prescriptions Outside of Expected Geographic Area

Drug diversion is the criminal act of unlawfully distributing prescription drugs. Drug-seeking and drug-selling enrollees commonly attempt to get narcotics, antidepressants, and antipsychotic drugs.

Drug seekers and sellers exhibit suspicious behaviors such as visiting multiple physicians or "doctor shopping," misrepresenting or presenting vague symptoms, and using multiple pharmacies. Many travel hundreds of miles and across state lines to get prescriptions and prescription drugs from "pill mills," which are doctors, clinics, or pharmacies that prescribe or dispense drugs inappropriately or for non-medical reasons. Drug diversion is often linked with identity theft, overprescribing physicians, and prescription theft or forgery.

If you suspect drug diversion, then think about contacting the CMS NBI MEDIC to find out whether an investigation is in progress on the enrollee, physicians and pharmacies involved.

5.4. Additional Resources

This section provides you additional CMS, policy/guidelines, data, and guidance resources. This type of information can be incorporated into your detection strategy as well as your prevention strategy.

5.4.1. Sources of Additional Information

CMS Resources

- CMS: cms.gov
- CMS Outreach and Education: cms.gov/Outreach-and-Education/Outreach-and-Education.html
- CMS Medicare-Medicaid Coordination: cms.gov/Medicare-Medicaid-Coordination/Medicare-MedicaidCoordination.html
- Medicare Parts C and D Recovery Audit Program: cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/recovery-audit-program-parts-c-and-d/index.html
- CMS Research, Statistics, Data and Systems: cms.gov/Research-Statistics-Data-and-Systems/Research-Statistics-Data-and-Systems.html
- Part C/Part D Contract and Enrollment Data: cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/MCRAdvPartDEnrolData/index.html?redirect=/MCRAdvPartDEnrolData/MACPC/list.asp
- HEDIS (Health Plan Employer Data and Information Set) Public Use Files: cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/MCRAdvPartDEnrolData/MA-HEDIS-Public-Use-Files.html
- CMS E-Prescribing: cms.gov/Medicare/E-Health/Eprescribing/index.html?redirect=/eprescribing

Medicare Coverage Resources

- Publication 100-16 MMCM: cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS019326.html
- Publication 100-18 Medicare PDBM: cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS050485.html
- Publication 100-01 Medicare General Information, Eligibility and Entitlement Manual: cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS050111.html
- Publication 100-02 Medicare Benefit Policy Manual: cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS012673.html
- Publication 100-03 Medicare National Coverage Determinations (NCD) Manual: cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS014961.html
- Publication 100-04 Medicare Claims Processing Manual: cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS018912.html
- Medicare Coverage Database: cms.gov/medicare-coverage-database

Other Medicare Contractors

- CMS NBI MEDIC: healthintegrity.org/contracts/nbi-medic
- CMS O&E MEDIC: medic-outreach.rainmakerssolutions.com/
- CMS Contacts Database: cms.gov/apps/contacts
- Coordination of Benefits: http://www.cms.gov/Medicare/Coordination-of-Benefits-and-Recovery/Coordination-of-Benefits-and-Recovery-Overview/Coordination-of-Benefits/Coordination-of-Benefits.html
- ZPICs/PSCs:
    - Zone 1: safeguard-servicesllc.com
    - Zone 2: healthintegrity.org/contracts/zpic-2
    - Zone 3: cahabasafeguard.com
    - Zone 4: healthintegrity.org/contracts/zpic-4
    - Zone 5: nciinc.com/about-us/advancemed
    - Zone 6: Not awarded at this time
    - Zone 7: safeguard-servicesllc.com
    - Eastern Benefit Integrity Support Center (EA-BISC) covers New York and New Jersey for Part A and Part B: safeguard-servicesllc.com/locations.asp

- New England Benefit Integrity Support Center (NEBISC) covers Medicare Part A including Home Health and Hospice, and Part B in Connecticut, Delaware, the District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, Rhode Island and Vermont: safeguard-servicesllc.com/locations.asp#ne
- NEBISC covers Home Health and Hospice in New Jersey, New York and Pennsylvania: safeguard-servicesllc.com/locations.asp#ne
- NEBISC covers only Part B in the County of Fairfax, the County of Arlington and the City of Alexandria in Virginia: safeguard-servicesllc.com/locations.asp#ne
- Pennsylvania Benefit Integrity Support Center (PENN-BISC) covers Pennsylvania for Part A and Part B: safeguard-servicesllc.com/locations.asp#penn
- DME PSCs for Jurisdiction A: tricenturion.com/

- Medicare Part D Recovery Audit Contractor: cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/recovery-audit-program-parts-c-and-d/Part-D-Recovery-Audit-Contractor.html
- Medicare Part D RAC Data Validation Contractor: cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/recovery-audit-program-parts-c-and-d/Part-D-RAC-DVC.html

Additional Resources

- Office of Inspector General (OIG) Compliance: oig.hhs.gov/compliance/
- OIG Fraud: oig.hhs.gov/fraud/
- OIG Corporate Integrity Agreements: oig.hhs.gov/compliance/corporate-integrity-agreements/index.asp
- FBI: fbi.gov/about-us/investigate/white_collar/health-care-fraud
- DEA: justice.gov/dea
- Stop Medicare Fraud: stopmedicarefraud.gov/index.html
- OIG database of excluded individuals/entities: oig.hhs.gov/exclusions/index.asp
- Excluded Parties List System (EPLS) on System for Award Management (SAM) website: sam.gov/portal/public/SAM
- Medicare Prescription Drug Benefit Model Guidelines: Drug Categories and Classes in Part D: www.usp.org/usp-healthcare-professionals/usp-medicare-model-guidelines
- National Institute of Standards and Technology: nist.gov/index.html

Public Information Resources

- Yellow Pages: yellowpages.com
- White Pages: whitepages.com

- AnyWho: anywho.com
- 411: 411.com

5.4.2. Complaint Handling

As noted in Section 5.1.1., complaints sponsors receive are excellent sources of data and intelligence regarding potential fraud. Complaints may cover a broad range of concerns, including Medicare sponsors, providers, Part D coverage, and the behavior of enrollees. A complaint may involve a grievance, an appeal, or a matter of coverage determination. A single complaint could include elements of all three.

Some complaints may allege that a provider, supplier, or enrollee received a Medicare benefit of monetary value, directly or indirectly, overtly or covertly, in cash or in kind, to which he or she is not entitled under current Medicare law, regulations, or policy. It is best practice for sponsors to treat these complaints as reports of potential fraud, whether or not the complainant identifies the activity as fraud, and to begin investigating.

Federal regulations[41] and the Compliance Program Guidelines specify the requirement for Part C and Part D sponsors to maintain documentation for each report of potential non-compliance or FWA. A complaint tracking system can help sponsors manage the information reported and assist with monitoring complaints for fraud.

Complaint Type. Complaints are typically of three types, as shown in the table below.

Complaint Type	Example
General concerns that can be addressed through the sponsor's complaint resolution procedures.	An enrollee calls to complain that he is dissatisfied with the list of providers available in his area.
Incidents of suspected fraud that need to be investigated.	An enrollee complains that for the past several months her pharmacy has only been dispensing 28 pills from a 30-day prescription for pain medicine.
Complaints that may initially seem to be general complaints, but further analysis might reveal a pattern of potential fraud (as explained below).	An enrollee calls to complain that he has tried repeatedly to contact a physical therapy clinic listed as a provider under his sponsor, but no one is answering the phone. Further analysis might lead the sponsor to suspect that this is a potential false-front provider.

Regardless of the complaint type, sponsors must follow the appropriate processes for addressing complaints. (See the MMCM, Chapter 13, for an in-depth discussion of grievances, appeals, and coverage determinations.)

Three aspects of complaint monitoring are particularly important to sponsors' fraud detection and prevention activities. These aspects are intake, tracking, and analysis.

[41] 42 CFR §§ 422.503(b)(4)(vi)(B) and 423.504(b)(4)(vi)(B)

Intake. Sponsors should have a formal process for documenting complaint intake regardless of the method of reporting (oral or written) or the initial identification as fraud (see Section 5.4.2. for information about complaint tracking). Include the following information when documenting the initial report of potential fraud:

- Date of complaint
- Information regarding the complainant (e.g., name and contact information)
- Information regarding the subject of the complaint (e.g., name, contact information, identifiers, type of service)
- Nature of complaint
- Brief description of complaint and any action taken to date

Sponsors should document this information in a standard way. The following two pages contain an example of a form that can be used for documenting complaint intake.

Sponsors need to begin investigation or referral activities for any complaints that indicate possible fraud. Other complaints or grievances can be handled through the appropriate processes that sponsors have developed internally.

SAMPLE COMPLAINT INTAKE FORM				
Assigned Complaint Tracking Number:		Title/Department:		
Recorded by:		Phone/Email:		
Complainant Information				
☐ Enrollee ☐ Provider ☐ Other :		If Enrollee, Applicable Coverage:		
Name:		ID #:		
Home Phone:		Cell Phone:		
Address:				
Email:				
Information Regarding Complaint				
☐ Complaint	☐ Provider Complaint	☐ Other Complaint:		
Name:				
Address:		City:	State:	ZIP:
SSN:	Medicare #:	Enrollee#:		
NPI #:	NCPDP #:	DEA #:	Other Identifier:	
☐ Part C	☐ Part D	☐ Part C and Part D		

Period of complaint:	Geographic Area Identified: ☐ Yes ☐ No If YES, Describe:	
Provider Type:		
☐ Adult Day Care	☐ Infusion Therapy	☐ Physician Specialty:
☐ Ambulance	☐ Laboratory	
☐ DME	☐ Mental/Behavioral Health	☐ Other Therapy
☐ HHA	☐ Outpatient Facility	Specify:
☐ Hospice	☐ Pharmacy	☐ Other
☐ Hospital	☐ Physical Therapy	If OTHER, Describe:
Complaint:		
☐ Address Change	☐ General Provider Complaint	☐ Quality of Care or Benefits
☐ Altered Claim	☐ Identity Theft	☐ Relationship with Provider
☐ Appeals Process	☐ Inactive Enrollee or Provider Number	☐ Service Accessibility
☐ Benefit Design	☐ Invoice Audit	☐ Services Not Rendered
☐ Claim Status	☐ Kickbacks/Bribes for Referrals	☐ State Notification Needed for Enrollee Status
☐ Co-Payment	☐ Enrollee in Wrong Region	☐ Timeliness
☐ Coverage	☐ Multiple MDs/Pharmacies	☐ Unbundling
☐ Difficulty Reaching Sponsor on Phone	☐ Not Medically Necessary	☐ Underutilization
☐ Double Billing	☐ Overprescribing	☐ Upcoding
☐ Drug Diversion	☐ Overutilization	☐ Other
☐ Enrollment/ Disenrollment	☐ Sponsor Communications	If OTHER, Describe:
☐ Excluded Drug	☐ Prescription Forgery	
☐ False-Front Provider	☐ Primary/Secondary Insurance	
Codes Identified:		
Brief Description of Complaint and Any Action Taken:		

Referred to:	☐ SIU	☐ CMS NBI MEDIC	☐ Other Law Enforcement	☐ Other Internal
Date Logged in Complaint Tracking System:				

Tracking. Establish a method for tracking all complaints, including allegations of fraud. Complaint tracking systems vary among sponsors and range from homegrown or vendor-developed software to spreadsheets maintained by a compliance management staff. Regardless of the scale and complexity, a tracking system can be an important tool in detecting fraud.

Tracking systems used successfully for fraud detection include the following capabilities:

- Mandatory fields that must contain data (such as the intake information listed above)
- Multiple sort and filter options, such as by:
    - Name of person or organization that is the subject of the complaint
    - Various identifying numbers (e.g., National Council for Prescription Drug Programs (NCPDP), NPI, DEA, sponsor, enrollee)
    - Date of incident
    - Geographic area
    - Complaint/suspected scheme type (e.g., drug diversion, services not rendered, identity theft, false-front provider)
    - Provider type

Sponsors need to use the information documented during complaint intake to populate the tracking system. The table below provides a sample list of data elements that are useful for tracking complaints.

Data Elements Related to the Complainant (If Known)		Data Elements Related to the Complaint Itself
Enrollee Caretaker ▪ Name/Anonymous ▪ Tracking # ▪ Medicare # ▪ Social Security # ▪ Enrollee Member ID # ▪ City ▪ State	**Provider** ▪ Name/Anonymous ▪ Tracking # NCPDP # ▪ NPI # ▪ DEA # ▪ Other ID # ▪ City ▪ State	▪ Part C or Part D ▪ Complaint/Scheme Type ▪ Brief Description of Complaint/Scheme ▪ Geographic Area Involved ▪ Provider Type Involved ▪ Billing Codes Identified ▪ Status

Analysis. The complaint tracking system is an active tool in fraud detection and prevention, not simply a repository for logging information. Rather, the system needs to be seen as an ongoing process in the fraud management life cycle.

Depending on the size of the sponsor and the average number of complaints received, sponsors should review the data in their claims tracking system on a regular basis to analyze the complaints and identify trends and patterns. These trends and patterns are important for identifying:

- Similarities among fraud cases that might indicate the spread of an existing scheme to a new geographic area
- Similarities among fraud cases that might indicate widespread criminal activity by a single individual or group that should be investigated as a single, large fraud case
- Evidence indicating that incidents originally categorized as general complaints and/or grievances are actually cases of potential fraud. This might lead to the discovery of a new scheme

Where sponsors identify new potential fraud cases, they should move that complaint into the processes for investigating fraud, including referral to the CMS's NBI MEDIC and/or law enforcement as instructed in the Compliance Program Guidelines.

Additional Resources

CMS has developed the Complaint Tracking Module (CTM) system for tracking and processing complaints received from enrollees and providers. The links below provide important information about the use of CTM, and CMS periodically releases reminders and prevention tips via HPMS:

- HPMS — Part C & Part D Program, CTM User's Manual (Plan Version): cms.gov/Medicare/Prescription-Drug-Coverage/PrescriptionDrugCovContra/Downloads/CTMPlansUserManual.pdf

- HPMS Memo — Updated CTM Guidance on Standard Operating Procedures: cms.gov/Medicare/Prescription-Drug-Coverage/PrescriptionDrugCovContra/Downloads/HPMSMemoCTMSOPUpdates_20110921FINAL.pdf

6. MITIGATION

No other sector of the economy has the specific mix of uncertainty, asymmetric information, and large numbers of dispersed entities that characterize the health sector. These features greatly increase the risk of fraud. They also make it difficult for sponsors to develop and implement corrective actions that reduce the potential for recurrence and ensure ongoing compliance with CMS requirements—mandated in federal regulations[42]—when fraud is detected or suspected within their networks:

- **Uncertainty**: Which enrollees will get sick or injured, when their health status will change, and how effective treatment options will be are all unknown variables. This uncertainty can make it hard to distinguish a fraud scheme from normal activity. It also makes it difficult to stop fraud perpetrators from setting up copycat fraudulent operations in new locations when sponsors and law enforcement identify a fraud scheme.
- **Asymmetric information**: The complex incentives healthcare providers face tempt some providers to reduce the quality of care, promote the use of unnecessary diagnostics or treatments, or even collaborate with criminal enterprises to perpetuate fraud schemes. Enrollees generally lack medical expertise so they rely on their providers' advice for making healthcare decisions. These two characteristics—diverging interests and incomplete information—greatly increase the risk for fraud and the difficulty of detecting and correcting it.
- **Geographically dispersed entities**: The presence of so many geographically dispersed FDRs in the health sector exacerbates the difficulties of generating and analyzing information, preventing fraud, and detecting and correcting it when it happens.

Because of the health sector's unique vulnerabilities to fraud, sponsors need to be reactive when the presence or a reasonable suspicion of fraudulent activity has been detected within their networks. Rapidly undertaking comprehensive mitigation and corrective actions is critical to reducing the potential for recurrence, ensuring ongoing compliance with CMS requirements, and helping safeguard other private and federal healthcare organizations and programs.

The section below describes how to comply with federal regulations[43] mandating Part C and Part D sponsors "adopt and implement an effective compliance program, which must include … measures that prevent, detect, and **correct** fraud, waste, and abuse." Based on these requirements, this section addresses strategies to take prompt action and reduce losses, identify root causes, develop corrective action plans, monitor corrective actions plans and actions, and retain records to support your efforts to correct FWA.

[42]42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

[43]42 CFR §§ 422.503(b)(4)(vi) and 423.504(b)(4)(vi)

6.1. Stopping Money from Going Out the Door

When you suspect or confirm your sponsor has improperly paid claims, you can take several immediate mitigation actions to stop more money from going out the door. This will help you avoid the "pay-and-chase" method of trying to recoup money after paying improper claims. Taking immediate mitigation actions can also help safeguard other private and federal healthcare organizations and programs.

Industry best practice immediate mitigation actions include:

- Stopping payment of claims when fraud is suspected. The prompt payment requirements set forth in the Medicare Improvements for Patients and Providers Act (MIPPA) of 2008 only apply to "clean claims"—claims that have no defect or impropriety. MIPPA allows sponsors to withhold payment until suspect claims have been investigated further to determine they are not fraudulent.

Industry Best Practice of Prepayment Review

An industry best practice is to stop money from going out the door to suspected fraudulent prescribers/providers through prepayment review. You could save millions when you put a problem prescriber/provider who files large claims on prepayment review.

- Subjecting future claims of prescribers/providers suspected of fraud to pre-payment review. Pre-payment review requires prescribers/providers suspected of fraud to file paper claims—rather than electronic ones—that clinicians and coders can process with special attention.
- Changing the member identification number of any enrollees whose identity may have been compromised.
- Reporting to the CMS NBI MEDIC and/or law enforcement any enrollees, prescribers/providers, or pharmacies whose identities have been compromised (see the CMS NBI MEDIC Compromised ID Form online at healthintegrity.org/docs/HI_MEDIC_Compromised_ID_Report_Form_20120515.pdf).
- Using data analytics (see Section 5.1.2.) to monitor all enrollees, prescribers/providers, or pharmacies associated with a suspected fraud scheme.

6.2. Identifying Root Causes and Taking Prompt Action

After taking immediate mitigation actions to stop money from going out the door, the next step is finding ways to correct improper behaviors to prevent similar fraudulent activity from happening within your network in the future. Per federal regulations,[44] you are required to correct fraud problems "promptly and thoroughly to reduce the potential for recurrence, and ensure ongoing compliance with CMS requirements," including conducting "appropriate corrective actions." In other words, whenever any of the types of Part C and Part D fraud activity described in Section 2.3. are discovered within your network, you are to take action to address the root causes, not just the symptoms, promptly and thoroughly.

[44] 42 CFR §§ 422.503(b)(4)(vi)(G)(2) and 423.504(b)(4)(vi)(G)(2)

Determining root causes requires answering a series of "why" questions and assessing the situation until the vulnerability that enabled the improper payment is found. This may involve creating a timeline with the data and evidence that identifies what should have happened versus what actually happened in the payment of a claim. It may also mean evaluating why the improper payments or suspect behavior went unnoticed when it first occurred and whether there were any failures to act due to the lack of requirements to act. Often, more than one corrective action is needed to deal with any single root cause. Corrective actions may involve FDRs or the sponsor itself.

6.2.1. Types of Corrective Actions for FDRs

Per federal regulations,[45] sponsors "must conduct a timely, reasonable inquiry," including an investigation, for suspected FWA. When your inquiry determines or reinforces your suspicion that an FDR is involved in fraudulent activity, you must conduct appropriate corrective actions to reduce the potential for recurrence of the FDR's deficiencies.[46] CMS strongly encourages sponsors to refer potential fraud to the NBI MEDIC and/or law enforcement.[47] Additionally, best practices in fraud fighting recommend that sponsors implement corrective action following any referral.

The following are types of corrective actions for FDRs:

- **Warning letters:** A warning letter is often the first corrective action to take against an FDR suspected of fraudulent activity. In the letter, detail what corrective actions you are requiring the FDR take in what time frame and the ramifications, such as contract termination, if the FDR fails to implement the corrective actions satisfactorily. To ensure an FDR is implementing any corrective actions you have mandated, conduct independent audits or review the FDR's monitoring or audit reports (see Section 6.3.).
- **Education materials:** Educational materials about Part C and Part D requirements can supplement the warning letter addressed above.
- **Requiring a corrective action plan:** In some cases, such as when widespread fraud has been detected through a CMS Fraud Alert (see text on CMS Fraud Alerts in Section 5.1.1.) or after repeated infractions, you may require an FDR to develop, implement, and monitor a formal corrective action plan. Section 6.3.4. includes a list of items that you can ask an FDR to include in its corrective action plan. In such a scenario, develop a written agreement for the FDR to review and sign detailing the corrective action plan; its timeline for specific achievements; and the ramifications, including termination, if it fails to implement and monitor the corrective action plan satisfactorily. More information on the requirements for written agreements is available in Section 6.3.5. Also, to comply with federal regulations,[48] you also must monitor implementation of the FDR's corrective action plan to ensure it is implemented effectively (see Section 6.3.).

[45] 42 CFR §§ 422.503(b)(4)(vi)(G) and 423.504(b)(4)(vi)(G)

[46] 42 CFR §§ 422.503(b)(4)(vi)(G) and 423.504(b)(4)(vi)(G)

[47] 42 CFR §§ 422.503(b)(4)(vi)(G) and 423.504(b)(4)(vi)(G)

[48] 42 CFR §§ 422.503(b)(4)(vi)(G)(2) and 423.504(b)(4)(vi)(G)(2)

- **Failure to take action**. When an FDR fails to implement satisfactorily the corrective actions specified in a warning letter or corrective action plan as described above, the next step is carrying out the appropriate disciplinary actions such as an overpayment or withholding payment you previously warned the FDR about in writing. Disciplining FDRs sends a clear message that fraudulent activity will not be tolerated.

6.2.2. Types of Corrective Actions for Sponsors

Corrective actions are often required to correct the root causes of behaviors in need of change and prevent similar fraudulent activity from occurring within your network in the future. Depending on the scale of any detected or suspected fraudulent activity, you may decide to undertake a few corrective actions or develop, implement, and monitor a formal corrective action plan (see Section 6.2.1. above). The following are types of corrective actions to think about.

Revision of Prevention Activities. Revising prevention activities is often key to ensuring similar fraudulent activity does not occur or go unnoticed in the future. Revising prevention activities includes:

- Revising your written policies, procedures, and standards (see Section 4.1.2.) and requiring employees and FDRs to review and sign them.
- Updating your system for routine monitoring, auditing, and risk assessment (see Section 4.1.4.)
- Increasing your collaboration with anti-fraud efforts, associations, and venues (see Section 4.3.)

Revision of Detection Activities. Revising detection activities is also often key to ensuring similar fraudulent activity does not occur or go unnoticed in the future. These types of corrective actions involve revising or expanding:

- Data sources and fraud indicators (see Section 5.1.1.)
- Data analytics (see Section 5.1.2.)
- Resources for data analysis (see Section 5.1.3.)
- Efforts to detect excluded/deceased providers and providers lacking credentials (see Section 5.2.)
- Efforts to detect abnormal patterns of prescribing/dispensing, missing provider identifiers, and high volumes of prescribing to enrollees outside of the expected geographic area (see Section 5.3.)

Corrections to Erroneous Data. Per the quality data reporting requirements in federal regulations,[49] sponsors are to develop, compile, evaluate, and report certain measures and other information to CMS, its enrollees, and the general public. When you detect fraud in your network, however, it is possible that the fraudulent activity has made some of this data erroneous.

To ensure your organization fully complies with CMS quality data reporting requirements, you typically need to implement corrective actions verifying and fully correcting your quality data in such areas as:

[49]42 CFR §§ 422.152(f) and 422.516(a)

- Cost of operations
- Patterns of utilization of services
- Developments in the health status of enrollees

Enrollee Fraud Aftercare. An industry best practice is instituting special administrative controls and quality-of-care checks to resolve the aftermath of fraud for enrollees. This practice ensures quality of care and enrollee safety. The following are examples of corrective actions to address enrollee needs when fraud has been identified:

- When fraud schemes involve services not rendered (see Section 2.3.1.), lack of medical necessity (see Section 2.3.2.), excessive services (see Section 2.3.3.), or controlled substances (see Section 2.3.6.), correct enrollees' medical and pharmaceutical claims histories as well as document plans to resolve any fraud-related health issues (e.g., opioids addiction, fraudulent medical records blocking enrollees from access to necessary services due to falsely exhausted calendar limits) and ensure standards of care are met moving forward.
- When fraud schemes involve identity theft (see Section 2.3.5.), correct enrollees' medical and pharmaceutical claims histories as well as take measures to help them recover from the ill effects of identity theft. At a minimum, this means changing their member IDs as an immediate mitigation action (see Section 6.1.). Other corrective measures may include mailing them educational materials about identity theft and Medicare consumer advocacy groups, monitoring their claims to deter future billings, and offering to enroll them in a credit monitoring service.

Payment Corrections. Federal regulations[50] mandate that you take corrective actions to identify overpayments and underpayments at any level within your network and properly report and repay those overpayments, where applicable.

You can combine your CMS enrollment data with your Prescription Drug Event (PDE) data to quickly identify and mitigate underpayments or overpayments before settlements are finalized. This type of data analytics is a fraud detection and payment corrections best practice for assessing the accuracy of PDE reconciliation data.

6.3. Developing Corrective Action Plans

Unlike immediate corrective actions (see Section 6.1. above), corrective action plans are longer-term and more strategic. They are designed to correct fraud or non-compliance promptly and thoroughly to reduce the potential for recurrence and ensure ongoing compliance with CMS requirements.

Besides fraud investigations, corrective action plan triggers can include the findings of an external or internal audit; compliance issues identified through routine internal risk assessments and performance monitoring; hotline or other reporting tool tips; and existing corrective action plan monitoring (prompting

[50] 42 CFR §§ 422.503(b)(4)(G)(2) and 423.504(b)(4)(vi)(G)(2)

a revision or new plan). Development and implementation of a corrective action plan involve eight steps as detailed below.

6.3.1. Step 1: Review of Situation

The first step in development of a corrective action plan is reviewing the situation to assess the magnitude of corresponding misconduct and non-compliance, particularly the risks to your sponsor and enrollees and the level of attention required to mitigate those risks. While this review will vary depending on the circumstances, it may be necessary to:

- Review the documentation for the situation prompting the corrective action plan and clarify the information provided
- Review previous fraud investigations and corrective action plans to verify each compliance problem is not a recurrence of a previous problem
- Think about whether the fraudulent activity pointed to systemic issues
- Analyze all of the circumstances related to the fraudulent activity, such as software, document handling procedures, equipment
- Gather additional evidence through site visits and/or interviews of the employees, FDRs, or enrollees involved

6.3.2. Step 2: Root Cause Analysis

To develop appropriate corrective actions, it is important to identify and understand the root causes that led to the fraud instead of simply reacting to the symptoms of the problem. As discussed in Section 6.2. above, root cause analysis involves asking "why" until you arrive at the fundamental cause of the fraudulent activity or non-compliance. You might also create a timeline of data and evidence and analyze each item to understand how the fraud occurred and why it went unnoticed.

6.3.3. Step 3: Identification of Corrective Actions

After you determine all the root causes, identify all the possible ways to correct and prevent similar fraudulent activity from happening in the future. Keep in mind:

- More than one corrective action is often needed to deal with any single root cause.
- There is no "one size fits all" corrective action. You need to give careful attention to what would be most effective in view of the specific root causes identified in your analysis.
- Corrective actions focused on collaboration with anti-fraud efforts, associations, and venues (see Section 4.3.) help safeguard other private and federal healthcare organizations and programs.

At the end of this step, a list of corrective actions (see Sections 6.2.1. and 6.2.2. for suggested corrective actions for FDRs and sponsors) is developed and ranked. In creating your final list, make sure to think about whether they:

- Address all the identified root causes (see Section 6.3.2. above)
- Cover all affected processes
- Are appropriate based on the degree of risk identified as part of your review of the situation in Step 1

Also, make sure that your final list of corrective actions does not adversely affect prompt payment of clean claims, enrollee quality of care, or enrollee safety.

6.3.4. Step 4: Development of Corrective Action Plan

The next step is development of a corrective action plan. Your corrective action plan may include:

- Description of the fraudulent activity expressed as a problem statement
- Background on the scope of the investigation
- Detailed description of how the corrective action plan will be implemented and monitored identified in Step 3 above
- Roles and responsibilities for execution of each action item, including the person responsible for completion of each action item
- Identification of the necessary resources (e.g., new software, staffing additions)
- Methods to monitor corrective actions and measure adherence to acceptable performance indicators (e.g., dashboards, scorecards, self-assessments)
- How any involved FDRs will satisfactorily complete the corrective actions and the ramifications if they do not complete them satisfactorily
- Measures to verify those involved FDRs adhere to applicable criminal, civil, and administrative laws going forward
- Escalation process for reporting to the CMS NBI MEDIC and/or law enforcement if suspect behavior continues
- Implementation schedule, including timelines
- The starting point for the transition from implementation to monitoring
- The end point for monitoring of your corrective action plan and/or integration into your routine monitoring, auditing, and risk assessment activities (see Section 4.1.4.)

6.3.5. Step 5: Signing of Written Agreements

After you develop your corrective action plan, you need to develop written agreements for FDRs who engaged in or are associated with suspect behavior. These FDRs are to review and sign the written agreements detailing the corrective actions they are required to take and the ramifications if they fail to implement them.

For FDRs, these written agreements also need to specify/reiterate they must:

- Maintain records on how they implemented and monitored corrective actions for a minimum of 10 years[51]
- Provide rights of access to these records to CMS or its designee[52]

6.3.6. Step 6: Implementation of Corrective Action Plan

The next step is implementing the corrective action plan and verifying each corrective action is initiated, completed, and documented. Each FDR assigned corrective actions in the plan needs to report the completion of all interim actions and steps regularly. They, in turn, need to confirm the interim actions and steps were completed as intended.

6.3.7. Step 7: Monitoring of Corrective Action Plan and Actions

You may monitor corrective actions during and after implementation to make sure your sponsor has effectively corrected issues associated with the suspect behavior and prevented reoccurrence. Monitoring corrective action plans and corrective actions can consist of performance data collection and analysis; independent audits or reviews of your FDRs' monitoring or audit reports; site visits; interviews of FDRs or enrollees; self-assessments; and the results of pre-payment reviews, post-payment reviews, or data analytics (see Section 5.1.2.). Monitoring activities typically occur within a set time frame and interval (e.g., three months, six months, one year).

Industry best practices include:

- Including processes in corrective action plans or corrective action plan policies and procedures to:
    - Escalate reports of unsatisfactory completion of corrective actions or projected unsatisfactory completion
    - Open new fraud investigations or make additional CMS NBI MEDIC and/or law enforcement referrals (see Section 8.1.) based on monitoring results

[51] 42 CFR §§ 422.504(a)(14)(d) – (e) and 423.505(d) – (e)

[52] 42 CFR §§ 422.504(a)(14)(d) – (e) and 423.505(d) – (e)

- Using metric reports and measurement tools (e.g., dashboards, scorecards, self-assessments) that can be integrated into your routine monitoring, auditing, and risk assessment, (see Section 4.1.4.) when the end point for monitoring your corrective action plan is reached to verify corrective actions result in sustained improvements in the long term

6.3.8. Step 8: Addressing Corrective Action Non-compliance

Through monitoring the corrective action plan, you may determine an FDR has not fully complied. Think about taking more aggressive action such as moving forward with an investigation or immediate referral to the CMS NBI MEDIC and/or law enforcement.

6.4. Retaining Records

Per federal regulations[53] and the Compliance Program Guidelines, your compliance officer is to maintain records about your organization's and your FDRs' corrective actions and corrective action plans, including how they were implemented and monitored, for a minimum of ten years. These federal regulatory requirements cover each report of potential fraud through any reporting method (e.g., hotline, mail, in person) whether the investigation resulted in corrective actions or not.

This documentation is to:

- Verify each corrective action was initiated, completed, and monitored
- Record the names and contact information for all the people who implemented and monitored the corrective actions (both employees and FDRs)

[53] 42 CFR §§ 422.504(a)(14)(d) – (e) and 423.505(d) – (e)

7. PRELIMINARY INVESTIGATION

The fraud management life cycle continues through the preliminary investigation process. A preliminary investigation is the triage of an allegation of fraud, waste or abuse identified through reactive (e.g., complaints, grievances) or proactive (e.g., data analysis, enrollment) means. The goal of a preliminary investigation is to determine if an allegation of FWA is credible and requires further investigation by the CMS NBI MEDIC or law enforcement and for you to take appropriate actions in an expeditious manner. This chapter will focus on preliminary investigative strategies, best practices, processes, and resources to assist in your investigative decision-making.

7.1. Investigative Strategies

To establish a preliminary investigative strategy, thoroughly evaluate the allegation through an initial review of the following components:

- Available internal and external documents/information
- Research results from public and commercial databases
- Complainant interview(s) (if applicable)
- Assessment of the loss to the sponsor and dollars at risk if the behavior continues

Focus on completing these actions as quickly as possible to triage the investigation.

Your overall assessment of the information gathered will help you determine if the investigation will move forward and will allow you to develop an investigative strategy tailored to the specific allegation and/or issue, including an expected completion date. The investigative strategy or plan will be similar for most investigations.

7.1.1. Timeliness

If you determine during the initial evaluation that the investigation will continue, it is most effective to move forward as quickly as possible through the investigative process to either refer the suspect to the CMS NBI MEDIC/law enforcement or take appropriate administrative action(s) such as an overpayment, payment withhold or pre-payment review edit. You may also determine during the triage or initial evaluation that you lack the appropriate resources or time to fully investigate the allegation; if so, immediately refer the suspect to the CMS NBI MEDIC or law enforcement. In this situation refer the investigation to the CMS NBI MEDIC or law enforcement within 30 days of identifying the allegation.

Once the CMS NBI MEDIC or law enforcement accepts your referral, they may require additional information to supplement the referral to support the investigation or future law enforcement requests for information (RFI). When the CMS NBI MEDIC sends you a request to support an RFI, respond to the request within 30 days. More severe issues are best addressed significantly sooner.

More information on this process is found in the Compliance Program Guidelines.

7.1.2. Dollar Thresholds and Combining Investigations

Assessing the total dollars at risk along with other factors assists with investigative workload prioritization, evaluation, and planning. During the preliminary investigation, it is helpful to review information such as billing data or to search historical files to determine a total loss to the sponsor due to the subject's actions. See Section 7.3. for additional information on prioritizing investigations based on a dollar threshold. A search of historical files or documents may include the following:

- Previous complaints
- Previous voluntary refunds
- Prior investigations
- Prior CMS NBI MEDIC referrals
- Previous direct education
- Previous CMS Fraud Alert (see text on CMS Fraud Alerts in Section 5.1.1.)

You might also find helpful information by researching your internal investigation tracking system (see Section 7.2.5. for information on investigation tracking) to ascertain if the subject has had previous investigations or shares patients or providers with other suspects under investigation.

It may also be beneficial to reach out to the CMS NBI MEDIC during the preliminary investigation stage to determine if the subject has had previous referrals from other sponsors. The CMS NBI MEDIC has the ability to combine cases relating to the subject into a regional or national investigation and significantly increase the total dollars at risk involved. Combining investigations with a larger dollar threshold ensures more law enforcement attention as well as a more efficient use of investigative resources.

Remember, however, that despite the importance of dollars at risk or previous aberrant behavior, they are not the only considerations in an investigation if there are also allegations of patient harm or abuse.

7.2. Investigative Best Practices

Preliminary investigation best practices include the following actions:

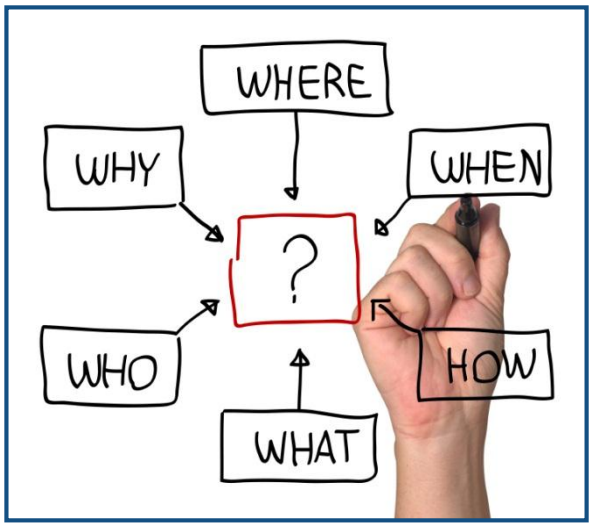
- Planning
- Collection of information and evidence
- Interviewing
- Document review
- Work paper development

The next sections will highlight these investigative best practices in more detail.

7.2.1. Planning

During the preliminary investigation phase, best practices recommend that you develop an investigative plan for each investigation. An investigative plan will keep the investigation on track and organized as well as maintain focus. It also ensures an efficient use of resources and prevents duplicate efforts.

The investigation plan may include the following elements:



- Allegation
- Source of allegation
- Assigned investigation priority
- Rationale for opening the investigation
- Action items/tasks for completion and projected time frames
- Possible information sources or resources to consult (e.g., subject matter experts, online databases, commercial databases)
- Expected completion date

The investigation plan should not take much time to develop and should be revised as you gather new information and facts.

Often the first action item or task for an investigator is to contact the source of the allegation. For example, if the source is an enrollee or current/former employee, the first step in your plan might be to contact the source for additional information. This will also help you determine the source's motive for reporting the suspect behavior.

The action items or tasks in the investigation plan will most likely include the following:

- Thorough background search and research
  - Online databases
  - Commercial databases
- Review of documents or information received via the source contact

Investigation Idea

If a provider files bankruptcy, compare the provider's billing to the bankruptcy discharge time frame if the provider is required to make payments. There may be a correlation if the provider's billing significantly increases during the same time frame.

Based on gathered information, your plan might also include one or both of the next steps:

- Perform a desk audit (cost efficient)
- Perform an on-site audit (interview staff and see day-to-day operations)

Your plan needs to consider the kinds of potential resolution or outcome action(s) that are likely as the investigation progresses. These resolution or outcome actions are specific to the investigation subject and knowledge you acquire during the preliminary investigative process. Resolution strategies may include one or more of the following (this is not an all-inclusive list of potential investigation resolutions):

- Close with no additional actions
- Monitor activity with no additional actions
- Direct education
- Direct education with pre-payment review
- Direct warning
- Refer to medical review
- Refer to provider outreach and education
- Overpayment/underpayment determination
- Referral to the CMS NBI MEDIC or law enforcement for further investigation

7.2.2. Collection of Information and Evidence

A major component of the investigative process is collecting reliable information based on credible sources of allegations, as well as material facts such as data analysis and background search results. It is crucial to document the collected information, records, or files and the related sources.

PIM exhibits provide examples of "reliable information":

- Documented statements from complaint or allegation sources that services were not rendered or misrepresented
- Signed attestations/statements from enrollees or current/former employees about the misconduct

- Peer comparison (focused data analysis) that distinguishes the investigation subject as an outlier
- Medical or document review obtained through pre-payment or post-payment review requests or site visits

The PIM exhibits also make the following key points:

- Credible information is material, meaning it supports the allegation by making the allegation of FWA plausible or probable.
- The term credible source describes someone who is "in the know" or has first-hand knowledge of an act or event. Sources are more credible if they have nothing to gain by making the allegation. Reliable information confirms that misconduct or behavior is likely not an error.

The preliminary investigative process does not carry the same burden of proof for a criminal or civil action. However, the information you collect will help you get reliable evidence that may later support a law enforcement case that results in civil or criminal activity.

Section 7.3., Investigative Processes, goes into the specifics of collecting and documenting reliable information.

7.2.3. Interviewing

During the preliminary investigation, you might consider an interview to help you to determine if an investigation is viable. The interview could lead you to the conclusion that the initial allegation is erroneous, that the complainant was confused about the billing, or that the investigation requires additional development. The interview may also indicate a direction for the investigation to take.

Interviewee Selection Tips

Interview individuals with direct or indirect knowledge of the following:

- Specific events
- Event/activity timelines
- Individuals involved
- Scheme emergence
- Additional contacts to interview

There are several different individuals, providers, or entities to consider interviewing in a preliminary investigation. Potential interviewees may include the following:

- Complainant
- Subject of investigation
- Other enrollees with billing by subject
- Other contacts obtained through the interview/investigation process
- Referral/prescribing sources

An interview provides a chance to get information from individuals with direct or indirect knowledge of the allegation. An interview also provides an opportunity to gain information and gather facts you otherwise would not know. You can use the interview to request additional information from the interviewee, such as copies of business license(s), medical license(s), equipment maintenance logs, inventory sheets, marketing materials, advertisement information, copies of treatment protocols, copies of agreements with vendors, and/or copies of subcontracts.

Interview recommendations and suggestions are addressed in more detail in Sections 7.3.1. and 7.3.2.

7.2.4. Document Review

The investigation process requires extensive research and information to support an allegation. Depending on the nature of the allegation, the research may extend to internal and external documents, Internet searches, or records from a provider or other source. Once the research and documents are collected, the investigative staff begins the evaluation of the information. This section highlights the types of information collected through the investigation and the review process. Sections 7.3.4., 7.3.6., 7.3.7., and 7.3.8. also address how to review the collected documents and information.

Examples of Investigative Documents. Documents gathered during the investigative process could include the following:

- Prepay medical records
- Post-pay medical records

- Registered agents
- Legal business name
- Corporation information
- Provider enrollment information
- Business license information
- Scope of practice
- Public database search information
- Commercial database search information
- Medical information
- Disciplinary actions

Examples of Sources of Investigative Documents. Investigative documents obtained through various methods could include the following:

- Prepay medical records request
- Post-pay medical records request
- Provider enrollment file
- Beneficiary enrollment file
- Public database search information
- Commercial database search information

It is helpful to establish formal and consistent processes to get additional records to support or disprove an allegation during an investigation. For example, it is generally best to establish a process that addresses public database searches (free online searches such as yellowpages.com) separately from commercial database (purchased searchable database such as LexisNexis) searches. A checklist with items that pertain to most investigations can simplify public database searches.

Examples of Public Database Information. Below are examples of the type of information found in public databases:

- Registered agent(s)
- Legal business name
- Related businesses with shared registered agent(s)
- Provider disciplinary action
- Specific provider type/specialty scope of practice

- Provider/medical license information
- Business license information
- Reverse address information
- Reverse telephone number information
- OIG Corporate Integrity Agreement
- Excluded individuals or entities

Due to the sensitivity of the information available in commercial databases, you might elect to designate an individual or specific team of individuals to perform these searches. Limiting those with access to commercial databases decreases the likelihood of misuse of this information, such as investigative staff accessing family member's information. Also, if there is a cost per search, limiting the number of employees who can run searches may help to contain costs.

Examples of Commercial Database Information. Below are examples of the type of information found in a commercial database:

- Name alias(es)
- Family associations
- Real property records
- Bankruptcy records
- Divorce records
- Division of motor vehicle information
- Social Security number verification
- Previous and current addresses
- Previous civil action
- Previous criminal action

Internal document requests, such as provider and/or beneficiary enrollment or information, are effective when included in the investigation file. Once you gather the investigative documents and search results, review for inconsistent or potentially falsified or altered information or documentation. An example is falsified liability insurance for a DME supplier.

For pre-payment or post-payment provider record requests, think about the following when creating a record request process:

Pre payment and Post payment Request Process	
Establish Processes to Determine How Many Enrollees' Records or How Many Claims to Request	1. Is a random pre-payment review edit for a specific provider the best approach? 2. Is a random sample of post-payment claims the best approach? 3. What time frame should you request records from? (e.g., dates of service or date of receipt for the last 12 months) 4. What type of services and/or items should be included in the request? Was the allegation centered on just one service or several?
Establish Response Time Parameters for Initial Pre-payment or Post-payment Requests	As an example, you may allow the subject 30 days to respond to the request.
Establish Response Time Parameters for Follow Up to Initial Pre-payment or Post-payment Requests	1. Will you give the subject 15 additional days? 2. Will you allow second or follow-up requests? 3. If no records are received, how will you proceed? Assume the subject has no records? Or will you make a third request?
Determine Types of Record(s) to Request Based on Provider Type/Specialty	Examples of records to request: ▪ History and physical notes ▪ Therapy notes ▪ Office visit notes ▪ Laboratory test results ▪ Delivery slips ▪ Inventory logs ▪ Drug invoices
Determine Which Type of Staff Will Review the Requested Records ***(Consider the potential that investigation/other staff who participate in the record review will be subject to a background check by a defense team if the investigation becomes a law enforcement case that goes to trial. Ensure staff is credible.)***	▪ Registered nurses and physicians for medical reviews ▪ Pharmacists for drug related reviews ▪ Subject matter experts ▪ Investigation staff/team
Implement a Decision Point After the Requested Records Are Reviewed	1. What types of issues or errors were identified? 2. Are the issues or errors medical necessity only? 3. Are the identified issues or errors indicators of FWA?

Pre payment and Post payment Request Process	
	4. If no indicators of FWA, does the investigation require additional review? 5. If indicators of FWA, is there still the need for additional investigation? Do you have the information necessary to conclude the investigation?
Document All Decisions and Findings	1. Document and summarize findings from the record review. Include incidents of missing records, potentially altered records, requested records that are missing specifically requested items, contradictory documentation, and/or contraindicated medical history. 2. Document rationale to proceed or not proceed with the investigation based on results of records review.

7.2.5. Work Paper Development

During the preliminary investigation process it is important to implement and maintain historical as well as current tracking of all investigations and associated information/documents. Investigation tracking ensures the accuracy of an investigation file and captures investigative logistics information, correspondence, communications, and all other associated actions with the investigation. Investigation tracking may be done through paper or electronic means. No matter how you track your investigation information think about including in your investigation tracking system the following elements, many of which are basic data that are obtained during the complaint intake process. (These elements were identified through industry best practices.)

Suggested Investigation Tracking Information	

Subject Information	▪ Name
	▪ Address
	  ○ Additional addresses, as necessary
	  ○ Phone numbers and other contact information
	▪ Subject Type:
	  ○ Provider
	  ○ Enrollee
	  ○ Referring provider
	  ○ Prescribing provider
	▪ Subject Sub-Type:
	  ○ Supplier
	  ○ Physician
	  ○ Mid-Level Practitioner
	  ○ Home Health
	  ○ Hospital
	  ○ Pharmacy
	▪ If appropriate:
	  ○ Billing Number(s)
	  ○ NPI(s)
	  ○ DEA
	  ○ UPIN

Allegation	▪ Summary or description of the allegation
	▪ Allegation type such as:
	  ○ Billing for services not rendered
	  ○ Upcoding
	  ○ Altered claims/records
	  ○ Unbundling
	  ○ Kickback/bribe
	▪ Source of the allegation:
	  ○ Enrollee
	  ○ Provider
	  ○ Current/Former Employee
	  ○ Anonymous
	▪ Source contact information:
	  ○ Name
	  ○ Address
	  ○ Telephone number
	  ○ Email address
	▪ Allegation time frame:
	  ○ Dates of service
	  ○ Claim receipt dates
	  ○ Paid dates

Identification Number	▪ Assigned investigation identification number
Investigation Status	▪ Pending ▪ Assigned/Active

Suggested Investigation Tracking Information	

	▪ Outcome/Resolution:
	  ○ Referral
	  ▪ CMS NBI MEDIC
	  ▪ Law enforcement
	  ▪ Department of Insurance
	  ○ Overpayment
	  ○ Voluntary refund
	  ○ Direct education
	  ○ Warning
	▪ Status date

Assigned Investigator/Analyst	▪ Name ▪ Title and organization ▪ Telephone number ▪ Fax number ▪ Email
Prioritization	▪ Assigned priority ▪ Date of assigned priority ▪ Updated/Revised priority ▪ Date of updated/revised priority

Documentation/ Narrative of Investigation Activity	Document investigative activities such as the following (best practice is to document the action within 48-72 hours of the action):
	▪ Billing information
	  ○ Billed/paid amounts
	  ○ Specific codes
	▪ Telephone conversations
	▪ Email contact
	▪ Correspondence
	▪ Educational contacts
	▪ Document request dates
	▪ Document source
	▪ Types of documents/information requested:
	  ○ EDI agreements
	  ○ EFT agreements
	  ○ Paper checks
	  ○ Copies of remittance advice
	  ○ Copies of paper claims
	  ○ Provider enrollment
	  ○ Beneficiary enrollment
	  ○ Open/closed appeals cases
	  ○ Open/closed overpayment cases
	  ○ Medical records
	  ○ Billing records
	  ○ Claims data or data analysis
	▪ Requested document response date

Suggested Investigation Tracking Information	

	▪ Record review outcomes/results
	▪ Site visit
	  ○ Date of visit
	  ○ Outcomes/results
	▪ Outcomes of previous investigations
	▪ Administrative actions
	  ○ Payment withhold
	  ○ Overpayment
	  ○ Negotiated settlement
	  ○ Prepayment review edits
	  ○ Internal referral to medical review or provider outreach
	▪ Interview(s)
	  ○ Interviewee contact information
	  ○ Date of interview
	  ○ Place of the interview
	  ○ Summary of interview

Along with the investigation tracking system, it is helpful to establish an investigation file order for working files so the associated correspondence and documents are quickly accessible. The file order should be flexible to handle electronic or paper associated investigative files. This ensures information gathered through the investigation process is well maintained. The sections and subsections listed below are an example investigation file structure:

Example Investigation File Order Sections/Sub Sections	
Investigation Information	▪ Investigation identification number ▪ Subject's name ▪ Subject's contact information
Investigation Origin	▪ Complaint or grievance (Reactive) ○ All additional complaints received after the initial ▪ Proactive referral from data analysis team, claims area, appeals area, any other intelligence source ▪ Previous investigations, complaints, grievances
Investigation Contacts	▪ List of sponsor's investigative staff/team that have direct knowledge of the investigation ▪ List of external contacts that have direct knowledge of the investigation (e.g., CMS NBI MEDIC contacts or law enforcement contacts)
Data	▪ Billing data ▪ Trending reports ▪ Peer comparison reports
Medical Review	▪ Medical records ▪ Review results summary ▪ Medical review findings per claim/enrollee

Example Investigation File Order Sections/Sub Sections	

Correspondence	▪ Internal document requests
	▪ Interview documents
	  ○ Complainant
	  ○ Provider
	  ○ Enrollee
	  ○ All other interviews related to the investigation
	▪ Medical review requests
	▪ RFI requests/responses
	▪ All other documents

Site Visit	▪ Provider interviews ▪ Staff interviews ▪ Enrollee interviews ▪ On-site request ▪ Record attestation ▪ Site visit summary ▪ Photographs
Provider Information	▪ Enrollment information ▪ EFT information ▪ EDI information
Referral Information	Copies of referrals to other entities such as ▪ CMS NBI MEDIC ▪ Law enforcement ▪ Department of Insurance

Administrative	▪ Overpayment
	  ○ Copies of overpayment demand letters
	  ○ Copies of claims spreadsheets used to determine overpayment
	  ○ Random sample documentation (if applicable)
	  ○ Extrapolated overpayment methodology (if applicable)
	  ○ Actual overpayment methodology
	▪ Education
	  ○ Copies of direct education material
	  ○ Summary information if education provided in a different format such as through a conference call or webinar
	▪ Pre-payment review
	  ○ Initial pre-pay edit request
	  ○ Pre-pay edit revision requests
	  ○ Pre-pay edit termination requests
	▪ Payment withhold requests or termination requests
	▪ Disenrollment
	  ○ Request for disenrollment
	  ○ Confirmation of disenrollment

Proper documentation of all investigative documentation/files activities (electronic or paper) ensures the chain of custody is maintained throughout the process. According to CMS, (see csrc.nist.gov/groups/SMA/fasp/documents/policy_procedure/Terms_Definitions_Acronyms.doc), chain of custody is defined as: A process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

As you document investigative activities remember to answer how, when, where, why, what and who about each document entered into the investigation file.

You may also establish an overall file and/or document retention process/policy for your investigative staff to address closed investigations and associated investigative files. Within your retention process, address file and/or document security to include how files are handled and maintained. Per federal regulations,[54] Part C and Part D sponsors will retain records, files and/or documents for at least 10 years. You may consider indefinitely retaining investigation files and associated investigative files to support ongoing investigations or potential civil/criminal actions (PIM, Chapter 4).

7.3. Investigative Processes

Throughout the investigation process, your main focus is to minimize the loss to the sponsor and protect the enrollees. Investigative tools vary based on the issue in an investigation.

Whether an investigation is identified through a reactive or proactive lead, there are key steps and tools necessary to substantiate an allegation and complete the investigation. The key steps and tools for an investigation include prioritization and evaluation of the information, as well as other investigative activities that will be highlighted in the following subsections. Also, think about having investigative staff meetings to manage the investigative workload as well as to address questions from the staff in case they need help with next steps.

The first step in the investigative process is to evaluate and prioritize the various investigations that may need to be pursued. Evaluation and prioritization allows you to make most productive use of limited investigative resources. The next table provides information on how you might prioritize.

Overall Prioritization Process
Intake the complaint and review the allegation.
Gather preliminary information: ▪ Review of previous complaints ▪ Provider enrollment information ▪ Review of previous education ▪ Review of previous medical reviews, education, and audits ▪ Initial data analysis to determine dollars at risk and items billed
Consider assigning prioritization points based on gathered information or previous knowledge of the subject (see suggested prioritization factors and scoring in the next table).
Document and file related prioritization information and documents.

[54] 42 CFR §§ 422.504(d) and 423.505(d)

Overall Prioritization Process

If you have a pending investigation workload, consider reprioritizing based on the following:

- Increased claims volume
- Increased dollars at risk
- CMS fraud alerts
- Additional complaints since the initial
- New intelligence from internal and/or external sources (see Section 5.1.1. for stakeholders)

Below are example investigation prioritization factors based on Compliance Program Guidelines and PIM, Chapter 4, and industry best practices with example scoring based on the preliminary investigation.

Prioritization Considerations and Example Point System	
Questions of patient harm, either financial or physical?	15 points
Previous complaints/identified issues?	10 points
Problem identified from CMS Fraud Alert (see text on CMS Fraud Alerts in Section 5.1.1.)?	5 points
Complaint made by internal/external stakeholders (reactive)?	10 points
Complaint originated through proactive means?	5 points
Is the provider a national provider?	5 points
Law enforcement request(s) for assistance?	5 points
Prior complaints with adverse findings?	10 points
Prior education?	5 points
Total number of enrollees?	Sponsors can evaluate their own data to identify thresholds.
Dollars at risk over the last 18 months?	Sponsors can evaluate their own data to identify thresholds.
Is billing behavior the same or similar to a known FWA scheme?	10 points
Total the points based on the information obtained during the preliminary investigation then assign to staff based on the prioritization score. (This is only an example of prioritization and your investigative staff/team may implement a different list of prioritization factors and scoring process appropriate for your organization.)	

The following table breaks down the overall steps involved in the investigative process.

Investigation Process Breakdown	
Prioritize the Investigation	See the table above for a suggested prioritization process and scoring.
Assign Investigation	After reviewing the complaint and billing involved, the management team (or other designated person) assigns the investigation to an investigator with previous experience with the identified issue or assigns an investigator without previous experience along with a mentor.
Preliminary or Ongoing Information Gathering ***(See Section 7.2.4. for additional suggested information sources)***	Information sources include: ▪ Investigation tracking system review for prior complaints, grievances and/or investigations ▪ Claims processing system review ▪ Corporate Integrity Agreement review ▪ Public Access to Court Electronic Records (PACER) online database review (bankruptcy activity) ▪ Claims data analysis/review ▪ Public internet database searches ▪ Commercial database searches ▪ Health Integrity and Protection Database (HIPDB) searches (if access is available)
Complaint Clarification (If Reactive)	Contact the complainant to clarify the information provided in the complaint.
Request Records	Request internal and external records* such as: ▪ Medical records to support billed services from provider for the claim in the complaint ▪ Billing records from provider ▪ Copies of EFT agreement(s) ▪ Paper checks (if not EFT) ▪ Copy of EDI agreement(s) ▪ Provider enrollment file ▪ Beneficiary enrollment file *Internal records are documents that your organization as on file and immediately available. External records are records that are not within your control such as provider records.
Determine Need for Site Visit	When determining the need for a site visit, think about the following: ▪ Potential for altered documentation ▪ Cost effectiveness of a site visit ▪ Priority of obtaining records ▪ History of complaints ▪ Need to verify provider is or is not at location or practice site that is listed on documentation ▪ Dollars at risk or financial loss data analysis or complainant information supports the allegation of aberrant billing behavior ▪ Provider has failed to submit records in the past upon request
Other Investigative Activities	▪ Determine the need for additional interviews ▪ Document dollars at risk ▪ Determine what data analysis is necessary (e.g., peer comparison or top-billed codes) ▪ Determine if there is a need to review additional claims beyond those that are the subject of the complaint

Investigation Process Breakdown	
Additional Records Request(s)	If you need to request additional medical records: ▪ Have investigative staff work with medical review staff to ensure all necessary records are requested based on the billing codes and policies/guidelines in effect for the billed items. ▪ Draft the records request letter that includes a response time frame. ▪ Verify the provider's address and contact information before sending the records request letter. Consider sending a modified patient list that contains the last name, date of service, and last five digits of the health insurance claim number (HICN). If the provider requests an extension to respond to the records request: ▪ Ask the provider to place the request in writing ▪ Respond with your decision in writing If you receive the requested records: ▪ Organize the records ▪ Verify receipt of all requested records ▪ Notify the review staff that records are ready for review
Record Review Results	Once the record review staff completes the review, meet as a team to review the documented results.
Determine Next Steps	Evaluate the information you find through the investigative process: ▪ Gathered information/documents/intelligence ▪ Complainant information ▪ Record review results ▪ Site visit information (if performed) ▪ Dollars at risk ▪ Additional interviews Based on your evaluation determine the most appropriate, effective outcome or resolution for this specific investigation. The outcome or resolution may include one or more of the following: ▪ Administrative actions ○ CMS NBI MEDIC and/or law enforcement referrals ○ Provider education ○ Overpayment ○ Payment withhold/suspension ○ Prepay edit(s) ○ Auto-deny edit(s) ▪ Direct referral to law enforcement
Investigative Resolution/ Outcome	▪ Notify the complainant of the outcome (depending on the organizations that become involved in the investigation, resolution may not occur immediately but over a significant time period such as months or years). ▪ Document resolution information. ▪ Organize final case file.

Sections 7.3.1. through 7.3.8. focus on additional processes that assist with development of an investigation. They are:

- Statements from anonymous and identified complainants
- Interviews with providers, enrollees, and others
- Data analytics review of individual complaints (overall patterns, trends, and errors)
- Document review (provider enrollment application, history and ownership; beneficiary enrollment application)
- Site visit
- Claims review
- Records and utilization review
- Financial and billing review

7.3.1. Statements from Anonymous and Identified Complainants

To strengthen your investigation, think about asking for a written statement from the complainant or interviewing the complainant as quickly as possible. This will give the complainant a chance to detail events, time frames, and involved individuals.

Below are example questions to ask during a complainant interview in the early stages of the investigation. (See Section 7.4.2. for more information on conducting interviews as part of your investigation, including example questions for a variety of interview subjects.)

Example Complainant Interview Questions
How did you find out about the activity?
Are there other potential contacts that are aware of the activity?
Do you have any papers, documents, or other items you can provide that support the allegation?
Do you know when the activity started? Is it still happening?

Some additional interview tips are below:

- Before you conduct the interview and while you are drafting interview questions, take into account the complainant's likely scope of knowledge and comprehension level (e.g., enrollee or enrollee's spouse versus a provider).
- Review contact information to make sure you have the best telephone number, email address, and physical address for the complainant. Be aware that the complainant may ask to remain anonymous.

If the complainant chooses to remain anonymous or asks not to be identified during the investigation, you may not have the chance to get additional information on the allegation. You may assign identification numbers to the anonymous complainant to mask his/her identity to maintain communication.

The risk with anonymous complainants who do not wish to have more than an initial contact is that without their cooperation the allegation may not be fully developed. A thorough initial complaint intake process will mitigate the risks with non-cooperating anonymous complainants by asking who, what, where, when, why and how. (See Section 5.4.2. for additional complaint intake information and guidance.)

7.3.2. Interviews with Providers, Enrollees, and Others

During the investigation process, you may determine an interview with a contracted provider, Medicare beneficiary, referring/prescribing source, or other individual may be necessary to support or disprove the initial allegation. From additional interviews you may be able to get information from individuals with direct or indirect knowledge of billing practices and event timelines, as well as the names of other individuals that may be involved in a FWA scheme or activity.

Your interviewees could include the following types of individuals:

- Subject of the investigation
- Medicare enrollee(s)
- Referring/prescribing source(s)
- Complainant(s)
- Additional enrollee(s) with the same billing by a provider under investigation
- Other contacts obtained through the interview/investigation process

Interview Tip

Before recording an interview, clear it with your legal counsel. Then clear it with the interviewee. The interviewee may request time to work with his/her legal counsel as well.

Before you schedule the interview, do as much background research on the interviewee and the allegation as possible. This ensures your focus is on gathering information/facts you did not already know or have prior to the interview.

Your research and/or the interviewee's specialty or facility type will assist you in developing interview questions. For example, a provider's billing practices/patterns may be included in the interview question development to ensure all potential issues are addressed. (See Section 7.4.2. for more information on conducting interviews as part of your investigation, including example questions for a variety of interview subjects.)

7.3.3. Data Analytics Review of Individual Complaints (Overall Patterns, Trends, and Errors)

Data analysis is essential in the evaluation of a reactive or proactive complaint or investigation to examine billing patterns, trends, and spike billing, and most importantly, to determine actual and potential loss to the sponsor. Complaint data analysis may start with a review of an enrollee's billing history or with an overall provider billing history to identify a potential FWA scheme. Consider implementing standard data analysis scripts that produce a series of reports for a specific provider or enrollee for a specified time frame (e.g., 18 months or two years).

Types of Initial Complaint Data Analysis: These are examples of the types of complaint development data analysis reports that may initially determine that the potential for FWA exists:

- Billing summary by year
- Total number of billed enrollees
- Top-billed codes
- Top-billed modifiers
- Top-billed place of service codes
- Total number of services by top codes
- Total referring/prescribing sources
- Average number of services per enrollee
- Average number of prescriptions per enrollee
- Average total paid per prescription per enrollee

If the initial data analysis appears to support the initial allegation, a higher level of data analysis is necessary to focus on a specific issue identified through the broader scope of the initial data analysis.

Types of Higher Level Complaint Data Analysis: Below are examples of data analysis that further characterize a FWA scheme:

- Review provider or enrollee billing history based on high-risk area (e.g., specific ZIP code or county in service area)
- Conduct peer comparison study (e.g., compare cardiologist's echocardiogram billing to all other cardiologists' echocardiogram billing within sponsor)
- Analyze unusual billing patterns/practices (e.g., only bill Evaluation and Management [E&M] code 99215)
- Assess spike billing reports (e.g., a significant increase in a policy group such as lab services may indicate a false-front or phantom provider)
- Examine billing shifts (e.g., a significant shift in billing behavior, such as when a DME supplier stops billing diabetic test strips and begins billing only spinal orthotics)

HHS OIG Recommended Data Analysis

The HHS OIG released two reports in June 2013 recommending Part D sponsors use PDE records for data analysis to identify suspect prescribers. One report focused on identifying individuals without the authority to prescribe and the other focused on identifying five types of prescriber outliers:

- High number of prescriptions per enrollee
- High number of associated pharmacies
- High percentage of Schedule II drugs
- High percentage of Schedule III drugs
- High percentage of brand-name drugs

For more information on these reports and their recommendations, please see Section 5.3.1. and 5.3.2.

- Perform overutilization/underutilization analysis (e.g., identify a high utilizing enrollee by the average number of Schedule II drugs purchased per month and compare this to the enrollee's previous 12 months of prescriptions)
- Compare geographic location of enrollees to the provider or broker/agent location
- Examine enrollees with multiple short-term enrollments with the sponsor

You may also identify new data analysis ideas or criteria from a Medicare Parts C and D Fraud Work Group meeting to implement in your data analysis program.

Overall, the best approach is to develop and focus your data analysis efforts to support complaint or investigation evaluation based on the nature of the allegation and then broaden the scope of the investigation as data analysis identifies other potential FWA issues. Data analysis may also determine there is no FWA issue and the complaint or investigation warrants no further development.

(Please see the Compliance Program Guidelines for additional information on data analysis as part of FWA detection and prevention.)

7.3.4. Document Review

As part of the preliminary investigation process you may need to request internal documents and/or information such as provider and beneficiary enrollment to validate an allegation.

Once you receive the requested enrollment information, begin a thorough review that includes verification of enrollment elements and identification of indicators of risky or suspect behavior. It is important to begin with the enrollment information because the submitted enrollment information may not be legitimate due to identity theft or the investigation subject may have intentionally provided incorrect information during the enrollment process.

The questions in the table below will help you detect suspect enrollment information relating to both providers and enrollees.

Questions/Indicators for Enrollment File Review		
1.	Is the enrollee located in a high-risk fraud area?	
2.	Are there original enrollee signatures or only copied signatures? (Consider comparing signatures to previously submitted documents.)	
3.	Was additional information/correspondence sent through email/mail during the enrollment process and not included with the original application?	
4.	Did someone other than the enrollee call with additional information during the enrollment process?	
5.	Are there markings, revisions, or indications of changes made with correction fluid on the application that are not initialed and dated by the enrollee?	
6.	Is the enrollee's only email address a "free" email account (if not enrollee)? (e.g., Hotmail, Gmail)	
7.	If paper information was submitted by the enrollee, does the postmark make sense compared to the enrollee's address?	
8.	Is the enrollee's only telephone number a "1-800" number?	
9.	Have you received multiple applications for the same enrollee?	
10.	Does information about the enrollee on social network(s) contradict the information provided on the application?	
11.	Is the provider under a Corporate Integrity Agreement (if not enrollee)? (See Section 7.4.1. for additional information.)	
Enrollee Specific		
1.	Is the enrollee able to easily verify his or her enrollment/sponsor change when interviewed or via written request/statement?	
2.	Is documentation of the scope of appointment available?	
3.	How did the individual enroll? (e.g., marketing event, individual contact)	

The provider enrollment file and related documents also provide an opportunity to identify related business associates, businesses, or addresses. As you find these during the review, check the related associates and addresses against public and commercial databases or reverse address/telephone searches. This layered search approach will assist with the proactive identification of other suspects to include in the investigation.

For a provider enrollment review, verify information or discrepancies found in the information through available online database or commercial database searches. The preliminary investigation process will allow you to verify/validate or identify contradictions pertaining to the following items (see Section 7.2.4. for additional items):

Verification Points/Discrepancy Indicators
Current license to practice or conduct business
Education and training records
Board certification in each reported specialty area (if required)
Original and/or copied signatures
DEA number
Social Security Number
EIN or tax identification number
Accreditation information (if required)
NPI number
Legal business name
Practice/Business address
Change of ownership not reported

You may also encounter unsolicited update and/or revision requests for a provider. This may indicate there may be an issue of identity theft, especially if the provider is not aware the request has been submitted. The list below highlights specific types of unsolicited requests for providers that may indicate suspect update/revision requests:

Suspect Update/Revision Requests
EIN or tax identification number updates
EFT change requests that include one of the following: ▪ Online only bank ▪ Bank is not in the same state as the enrollee ▪ Bank is 50 or greater miles away from the enrollee's location ▪ Bank is out of the country ▪ Bank account number update or revision
EDI change requests
Address changes or adding locations that are greater than 50 miles away from the provider's current location or have a post office box or mail service as a location
Website address change but the original website is still available
Contact information changes to include: ▪ Email address updates to free email accounts ▪ Telephone number updates to cell telephone numbers

Suspect Update/Revision Requests
▪ Correspondence address update that is more than 50 miles from the enrollee's current address or out of the state
EDI information (electronic claim submitter information)and billing redirection to a new submitter identification number
Electronic/paper remittance redirection to a new vendor/correspondence address

Additional indicators to detect false-front providers or identity theft may also include the following:

- Returned mail due to a non-existent correspondence address or because no one at the address knows the recipient
- Addresses that correspond with commercial mailbox facilities (FedEx, UPS)
- Email that kicked back due to an invalid email address or closed email account
- Disconnected or out-of-service telephone numbers
- Provider's EFT does not successfully complete

If you suspect provider or enrollee identity theft during the preliminary investigation process, think about following this process to prevent the identity theft from continuing:

1. Contact the provider or enrollee to verify if he/or she initiated the enrollment or revisions.
    a. Document verbal statements and follow up with a written summary to the provider or enrollee.
    b. Or, send a written statement to the provider or enrollee and request a signature to confirm the discussion or information.
2. If the provider or enrollee has not notified the CMS NBI MEDIC to request inclusion in the Compromised Number Contractor (CNC) database, notify the CMS NBI MEDIC of the suspected identity theft.
3. Then, implement a pre-pay or auto-deny edit or withhold payment based on the provider or enrollee's specific situation. (You may check with your CMS Account Manager prior to implementing these types of edits.)

Document and flag all discrepancies identified through the enrollment file or document review in your investigation tracking system as discussed above. This type of information is important to determine if the investigation warrants referral to the CMS NBI MEDIC and/or law enforcement for additional investigation or administrative actions only.

7.3.5. Site Visit

A site visit may be necessary during the preliminary investigation phase if the allegation contains indications of the following:

- Altered medical or billing records/documents
- Potential of altered medical or billing records/documents
- No medical or billing records/documents exist
- Question if the provider exists

Contact with the complainant will reinforce if a site visit is necessary based on his/her direct knowledge of the situation.

Site Visit Tips

- Do not accept anything from a suspect while conducting a site visit, including food, drink, or office supplies. This prevents allegations of impropriety by the site team visit.
- Do not discuss the suspect or how the site visit is developing when left alone in the suspect's office or facility. Even when you think you are alone, surveillance or security equipment may be recording.

Consider that site visits are an expensive method to retrieve medical and business records from a suspect; however, they may be necessary to support an allegation. In deciding whether or not to conduct a site visit, review the suspect's overall history to determine total risk.

If you determine a site visit is necessary, the next step is to decide if an announced or unannounced site visit is appropriate. Allegations of altered or non-existent records and/or a potential false-front are best investigated with an unannounced site visit. If an unannounced site visit is the best option based on the allegation, notify the appropriate internal (e.g., legal counsel, compliance) and external (CMS NBI MEDIC, CMS, law enforcement) entities before you conduct the unannounced site visit. An unannounced site visit prevents the subject from fabricating or altering records or coordinating with other suspects prior to your arrival. The table below provides suggested steps to prepare for an unannounced site visit.

Send the unannounced site visit request or discuss with the CMS NBI MEDIC and/or law enforcement to ensure the action will not interfere with an ongoing CMS NBI MEDIC or law enforcement investigation.

If an unannounced site visit is not viable, an announced site visit is the other option. In addition to the unannounced site visit steps outlined above, you will want to determine an acceptable form of notice to the provider regarding the site visit and a time frame (e.g., notify the provider within 10 minutes of your estimated arrival at the provider's office or fax a site visit notice to the provider within an hour before your visit).

Whether your visit is announced or unannounced, you will need to be prepared for the site visit. As you plan the site visit, take the following into account:

Site Visit Planning	
Determine the Type of Staff to Conduct the Site Visit	The type of the provider involved may call for a site visit team consisting of a range of skills: ▪ Fraud investigation ▪ Subject matter expert(s) (managed care, DME) ▪ Medical personnel (MD, RN, PT) ▪ Pharmacists ▪ Billers and coders ▪ Accountants
Distinguish Roles for the Site Visit Team	▪ Designate a senior team member to lead the interview and respond to questions from the subject and/or subject's staff ○ Assign a team that consists of at least two members ▪ Designate a note taker ▪ Designate a team member to observe: ○ Subject and/or subject's staff behavior ○ Posted documents or advertisement materials that are clearly visible ○ Subject's staff copying or electronic identification of requested records
Determine Equipment/Supplies Needed to Conduct the Site Visit	Example equipment/supplies: ▪ Encrypted laptop computers ▪ Cellular phones ▪ Tape recorder ▪ Camera ▪ Portable scanner ▪ Portable copier ▪ GPS unit ▪ Mailing supplies ▪ File folders ▪ Pens, pencils, paper, Post-it notes
Business Identification	Be prepared with: ▪ Business cards ▪ Business picture identification badge/card ▪ Introduction letter to explain who/why you are there
Office Contact	Designate an investigative staff member to assist the site visit team while they are in the field with things such as: ▪ Directions ▪ Additional data analysis ▪ Copies of letters ▪ Copies of educational information
Travel Coordination and Arrangements	Coordinate investigative staff site visit travel. There may be additional providers or enrollees that require a visit that are not related to your investigation. However, this type of coordination is an efficient use of time and resources.

Site Visit Planning	

Site Visit Documents	▪ Interview questions:
	  ○ Prepare interview questions
	  ○ Site visit staff should review the interview questions to ensure understanding
	▪ Records request letter.
	▪ Enrollee or claim list attachment(s) for record request letter.
	▪ Medical records attestation form that asks the provider to sign agreeing all requested records have been provided in full. Recognize that the provider is not required to sign, in which case be prepared to have a senior team member annotate the letter with the statement that the provider makes as to the rationale for not signing. This annotation needs to be dated and signed by the individual making the annotation.
	▪ Authorization form to take documents offsite in case the provider does not have equipment to copy/scan records or you do not have a sufficient portable copier/scanner capacity.

Safety Assessment	Ascertain if there are any known safety issues before conducting the site visit and during its conduct.

Once you are ready to conduct the site visit, the following suggested protocol will ensure a successful and complete site visit:

Site Visit Activities
Develop a pre-interview site visit assessment based on the preliminary planning and analysis you have done per the recommendations above
Evaluate the safety of going into the location. Example indicators to look for: ▪ Is it a legitimate business office? ▪ Is it clearly marked as a business? ▪ Are there people loitering in the parking area? ▪ Go with your instinct on entering the location
If applicable, clearly identify yourself as sponsor investigative staff, not law enforcement, as you begin the site visit: ▪ Take pictures of the exterior of the office or facility ▪ Note the time the site visit begins ▪ Ensure that your entire site visit team has the records request letter and business cards ▪ Ensure your identification is visible ▪ Explain the purpose of the site visit ▪ Ask for the appropriate staff member(s) to work with
Once the appropriate staff member(s) is identified, begin the following: ▪ Conduct entrance meeting with the provider and provider staff to explain how the site visit process will work. ▪ Provide your business card to the subject as well as other office personnel such as administrative staff. (Staff may call you later with additional information he/she would not provide during the site visit.)

Site Visit Activities
▪ Begin the retrieval of the requested records. ▪ Ask for copies of other records like equipment maintenance logs or advertisement/marketing material (as necessary). ▪ Ask for a tour of the office or facility. ▪ Ask to see equipment used to perform tests or procedures, as appropriate based on billing history and provider specialty. ▪ Take interior pictures as permitted. Do not include patients in the pictures. ▪ Interview the provider and provider staff. ▪ Interview operational or business managers such as the Billing Manager or Office Manager to ensure a good overview of how the office or facility operates.
As you prepare to exit the site visit location: ▪ Conduct an exit meeting with the provider and/or provider staff. You do not need to provide any information on your findings or conclusions. ▪ Verify contact information of the provider and provider staff interviewed or involved in the site visit. ▪ Obtain business cards from the provider and provider staff involved in the site visit (if possible). ▪ Note the time the site visit ends. ▪ Ship obtained records via appropriate mail service if you are not returning to your office site. (If the records contain PHI, the records should be sealed/secured and remain in your possession or shipped via Certified USPS mail.)

After the site visit is completed, you may want to conduct the following post site visit activities within 48-72 hours to ensure accurate documentation and follow up on any identified clarification questions for the provider or provider staff:

Post Site Visit Activities
Formally document interview responses
Document all site visit activities
Send copy of scanned or copied records to provider with an attestation form to request the provider's signature and agreement that the scanned or copied records are correct
Document receipt of the attestation from the provider

In addition, schedule and hold a site visit team debrief meeting with other investigative staff to discuss best practices and lessons learned from the site visit. This will improve and refine your overall site visit process.

7.3.6. Claims Review

Claims review is a component of the preliminary investigation that assists in the determination of potential aberrant or incorrect payments. Claims review can establish if there is a loss to the sponsor or identify a much larger billing scheme.

There are several ways to review claims. These include the following:

- Review of single claims
- Claims processing system edits: pre-payment review, auto-deny or utilization
- Post-payment review
- Data analysis

This following section will provide examples of each of the above types of claim review.

Review of single claims. When you begin a claims review during a preliminary investigation, start with the claims processing system. As you review a single claim in question, ask yourself questions such as:

Single Claims Review Questions to Ask
Was the claim in question submitted and paid or denied? The submitted claim establishes loss or an attempt to be reimbursed.
Did the enrollee already receive a same or similar item/service from a different provider?
Has the enrollee received items/services from the provider before?
Does the enrollee's billing history support that he/she would need the service/item?

Claims processing system edits. Requesting special claims processing edits is an effective means of minimizing loss to the sponsor while you investigate an allegation or an effective administrative action. You can use claims processing system edits to get records, monitor billing, or protect providers and/or enrollees in a real time environment. (Consult your CMS Account Manager before implementing these types of edits.)

If you determine the preliminary investigation requires additional claims review, request records via a pre-pay edit with a narrow scope (e.g., specific billing code for a specific enrollee) based on the allegation. Pre-payment review will allow you to review real time provider claims/records and make a decision before the claim is adjudicated.

To establish a pre-payment review edit, define the type of claims you want to review based on specific claims criteria and suspects. Below are examples of the type of criteria you may include in a pre-payment review edit:

Example Pre payment Edit Criteria
Specific HICN/Sponsor member identification number
Specific National Provider Identification (NPI)number
Specific referring/prescribing NPI, DEA
Provider specialty type
Date range(s) (Date of service, date of receipt)
Billing code(s)
Diagnosis codes
Type of bill, revenue codes, condition codes
Place of service code

The following are example pre-payment edits with specific claims criteria:

- Specific provider billing number for billing code range 99212-99215 for dates of receipt on or after 06/01/2012
- Specific HICN or sponsor member identification number only for dates of service 05/01/2012 through 08/31/2012
- Specific referring physician for HCPCS K0823 for dates of receipt on or after 05/01/2012

Utilization edits are effective for an investigation when there is a question of over- or underutilization of services/items. These edits allow you to:

- Deny services/items that exceed policy (e.g., enrollee is receiving 600 intermittent catheters per month from four suppliers, but does not know why. The utilization edit will only pay 200 intermittent catheters regardless of the number of billing suppliers.)
- Identify or trend claims for excessive controlled substances for a specific enrollee
- Apply limits on the number of times a prescription can be refilled for a specific enrollee for a specific prescribing source

If you determine through the preliminary investigation, a provider, enrollee, and/or referring/prescribing source is the victim of identity theft, an auto-deny edit may be the most effective way to stop the loss and the fraud from continuing. The allegation and your investigative development help determine how the edit will be implemented. The following are examples of auto-deny edits related to potential identity theft:

- Deny all billed A4253 (diabetic test strips) for specific enrollee for specific provider for all dates of service
- Deny all services referred or prescribed for specific enrollee for all claims received on or after 05/01/2012
- Deny all services submitted by a specific provider for a specific enrollee for all dates of service

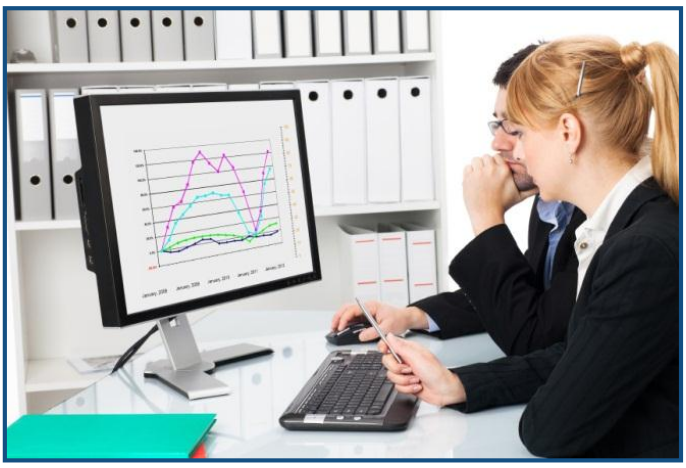
Use claims processing system reports to monitor the edit results and outcomes to support your investigation by accumulating billing data and review findings. Adjust or terminate the edits as needed.

Post-payment review. This is another type of review that will allow you to review a claim after it has been adjudicated. Post-pay review is important if you think there is likelihood of inappropriate claims and data analysis has established a potentially suspect pattern of behavior.

Data analysis. This is another means of high-level claims review for a preliminary investigation. Data analysis allows you to focus on a specified time frame (e.g., 18 months, two years) for a specific investigative subject as well as continue to monitor a subject's billing during an investigation.

The advantage of using data analysis for claims review is the immediate identification of a suspect or aberrant billing pattern/practice within a preliminary investigation. Quick identification allows you to move forward more rapidly with an investigation resolution and/or outcome. For examples of data analysis, see Section 7.3.3.

Overall, each investigation requires a different approach based on the nature of the allegation. However, the methods described above provide you with an in-depth review and analysis of records and claims data.



7.3.7. Records and Utilization Review

During an investigation the focus of medical and other treatment records review is to substantiate or disprove an allegation. The table below provides a breakdown of the decision-making process to request records:

Example Decision Making Process for Record Request(s)	
Do You Need to Request Records? •	Records review provides information related to billing and coding, as well as any potential for patient safety issues. Based on the information you get during the investigation you may need additional records to substantiate the allegation.
From Whom Should I Request Records?	Example record sources: ▪ Billing provider ▪ Referring/prescribing source ▪ Certifying provider Ultimately, you may need records from more than one source (e.g., request records from a DME provider and the referring provider for DME).
What Records Does the Provider(s) or Referring/Prescribing Source Have to Produce?	Review the provider's contract to determine records submission requirements. Consider both pre-pay and post-pay records.
How Many Records Do You Need to Request?	Based on your investigative research: ▪ Determine if you only require records for the claim in question, or determine if you require several claims with supporting records to see if there is a pattern of behavior ▪ Will you use a statistically valid random sample (SVRS)? Will you use a random number generator?
How Should You Obtain the Records? *(See Section 7.2.4. for more information on record requests and response time frames.)*	▪ Record request letter with specific response time frame sent via secure fax or registered/certified mail ▪ Potential site visit if there are concerns the provider may alter or fabricate records

Example Decision Making Process for Record Request(s)	
Who Will Review the Records?	Depending on the type of provider or specialty, assign review staff that has expertise and certification (as required) in that area if possible. Example subject matter experts: ▪ Medical director ▪ Pharmacist ▪ Registered nurse ▪ Licensed practical nurse ▪ Physical therapist and other specialty therapist Pharmacist: ▪ Contract identified subject matter expert ▪ Certified coder
After Obtaining the Records, What Is Next? *(See Section 7.2.4. for more information on record review summary and findings information.)*	▪ Copy or scan the received records to preserve the information. ▪ Use the scanned or copied version of the received records for review. ▪ Forward in a secure manner to review staff/team to complete the record review. ▪ Reviewer completes the review and provides: ○ Summary of findings ○ Documented each inconsistency or potential issue

Since the purpose of the records review is to identify potential FWA issues, the focus of the review is on inconsistencies, potential alterations, or contradictions in the records. It is important the assigned review staff/team fully understands the original allegation and future investigative findings.

Consider scheduling an investigative and review staff/team meeting prior to commencing with the record review to ensure all have the same understanding and focus. Before the record review staff/team begins the review, think about the following:

- Confirm the provider is licensed or certified to provide all billed items/services within the review.
- Identify all associated rules, regulations, and policies for billed items/services.
- Determine if records are in compliance with or meet applicable Medicare rules and regulations.
- Determine if the provider is following recognized standards of medical practice or accreditation guidelines.

The following list provides examples of potential fraud issues you may find during a fraud-focused records review:

Potential Fraud Issues You May Find during a Fraud Focused Records Review
Original ink appears to be present on copied records
Correction fluid appears to be present on copied records
Sections of the record(s) have been blacked out or removed

Potential Fraud Issues You May Find during a Fraud Focused Records Review
Records contain the same or similar verbiage for each patient (cloning)
Strike-through without the provider's initials and date for confirmation
Record appears to be back dated to cover a service time frame
Inconsistent or illegible provider signatures within the record(s)
No provider signature throughout the record(s)
Provider's electronic signature is the same date as your record request
Records are missing consecutive pages
Record contains added correspondence from the provider to explain why the service was billed
Notes have been added to the record months after the date of service (date/time stamp or written entries)
For equipment, the serial number is the same on all of the delivery slips

To ensure your record review is comprehensive, request records that are specific to the provider, specialty, billed items/service, applicable rules/regulations/policy, and the allegation.

Below are example record requests for a DME and home health provider:

Example DME Records Request for Diabetic Supplies	Example Home Health Records Request
▪ Documentation of dispensing order ▪ Detailed written order ▪ Enrollee authorization ▪ Proof of delivery ▪ Refill requests with enrollee response documentation ▪ Recorded phone conversations with the enrollee, if available ▪ Pick-up slips and /or documentation the equipment or supplies were returned ▪ Medical records to substantiate the need for the billed equipment/supplies ▪ Documentation of attempts to collect any deductible and/or coinsurance ▪ If unable to collect co-payment, documentation of financial hardship ▪ Documentation of enrollee contact or complaints with resolution information ▪ All other documentation to support the billed service(s)	▪ All Outcome & Assessment Information Set (OASIS) completed during the period under review (e.g., admission, recertification) ▪ Physician Plan of Care/Certification/Recertification (CMS Form 485) ▪ Supplemental orders ▪ History and physical ▪ Hospital discharge summary, if applicable ▪ Admission notes ▪ Discharge notes ▪ Nursing progress notes ▪ Therapy (physical, occupational and/or speech therapy) evaluation(s), plan(s) of care and notes ▪ Home health aide notes ▪ Social worker notes ▪ Supervisor visits ▪ Laboratory results ▪ Medication sheets ▪ Patient roster ▪ Consent for treatment ▪ All other documentation to support billed services

Regardless of the provider type or items/services billed, think about asking for the following items:

- Signature cards for the provider for comparison during the record review
- Example of full name signature
- Example of initials
- All other aliases/forms of signature
- Explanation of electronic records system to include the date and time stamp process

During the review consider comparing the billed claims data to the records for verification, keeping in mind the following questions (this is not an exhaustive list):

- Do the records support excessive or under-utilized items/services?
- Do the billed drug units match the billed drug code units?
- Is the billed diagnosis code supported by the records?
- Are the drugs prescribed supported by the diagnostic codes?
- Is the level of the billed service supported by the records?
- Do the records support the number of miles traveled?
- Do the records support the number of minutes billed?

Consider comparing the records and claims information to the enrollee's claims history in the claims processing system:

- How many other providers have billed the same or similar item/service in a similar time period for the enrollee?
- Does the enrollee's claims history confirm the billed condition?

After the record review is complete, the review staff/team may summarize as well as categorize the findings (e.g., 75% of the reviewed records indicated infusion therapy for enrollees with only E&M diagnostic codes). Categorizing and summarizing findings establishes a pattern or trend of behavior within the reviewed records. The pattern or trend distinguishes a mistake from potential fraud.

Consider implementing an error threshold or benchmark such as at least 60% of the records contained same or similar issues. The threshold could be your guide as to your next investigative steps:

- If the error rate exceeds the threshold this may indicate a referral to the CMS NBI MEDIC or law enforcement.
- If the error rate is below the threshold this may indicate administrative actions.

7.3.8. Financial and Billing Review

The preliminary investigation may require a review of billing or financial records to support or disprove an allegation.

Analysis of patterns of claims submission and payment information may detect suspect billing patterns or behavior. Financial and billing information provides an overall view of a subject's business and day-to-day operations. The following questions are helpful for reviewing billing or claim submission information:

Billing or Claim Submission Questions	
How Often Does the Provider Submit Claims?	▪ Daily ▪ Once a week ▪ Once per month ▪ Twice a week
Does the Provider Use a Billing Vendor to Submit Claims?	Request EDI agreement to confirm business agreement and submitter ID.
Does the Provider's Billing Vendor Also Submit Claims for Other Sponsor Providers?	Request a list of other providers associated with billing vendor.
Run Data Analysis to Identify Provider and/or Billing Vendor Patterns and Behavior.	Look for: ▪ The same items/services across all clients ▪ The same billed amount per items/services per client ▪ The same referring/prescribing sources across all clients ▪ The same enrollees across all clients regardless of benefit type ▪ High volumes of claims billed (e.g., bills 500 claims once a week)
How Does the Provider Receive Reimbursement or Payment?	▪ Paper checks ▪ Electronic funds transfer (If electronic, request a copy of the provider's EFT agreement.)
How Often Does the Provider Receive Reimbursement or Payment?	▪ Once per day ▪ Once per week ▪ Once a month
How Does the Provider Receive Remittance Advice?	▪ Electronic remittance advice ▪ Paper remittance advice

In addition, consider requesting financial records as part of a records request if the allegation includes a potential routine waiver of co-payments. Ask the provider for the following types of information when addressing routing waiver of co-payments:

- Copy of collection process for all enrollees
- Copies of attempts to collect co-payments from a specific enrollee or enrollees

- Copies of correspondence with the enrollee related to attempts to collect
- Copies of billing staff notes that document conversations with enrollees related to attempts to collect
- Copies of documentation from an enrollee addressing reason he/she cannot pay the co-payment

Financial or billing records will document a pattern of behavior or show the provider applies a hardship policy in specific situations.

7.4. Resources

This section provides additional CMS, policy/guidelines, data and investigative resources.

7.4.1. Helpful Websites

CMS Resources

- CMS: cms.gov
- Parts C and D Recovery Audit Program: cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/recovery-audit-program-parts-c-and-d/index.html
- CMS E-Prescribing: cms.gov/Medicare/E-Health/Eprescribing/index.html?redirect=/eprescribing

Medicare Coverage Resources

- Publication 100-08 Medicare Program Integrity Manual: cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS019033.html
- Publication 100-16 MMCM: cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS019326.html
- Publication 100-18 Medicare PDBM: cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs-Items/CMS050485.html
- Medicare Coverage Database: cms.gov/medicare-coverage-database/
- CMS Information Security Terms, Definitions, and Acronyms: csrc.nist.gov/groups/SMA/fasp/documents/policy_procedure/Terms_Definitions_Acronyms.doc

Other Medicare Contractors

- CMS NBI MEDIC: healthintegrity.org/contracts/nbi-medic
- CMS O&E MEDIC: medic-outreach.rainmakerssolutions.com/
- CMS Contacts Database: cms.gov/apps/contacts
- ZPICs/PSCs
    - Zone 1: safeguard-servicesllc.com
    - Zone 2: healthintegrity.org/contracts/zpic-2

- Zone 3: cahabasafeguard.com
- Zone 4: healthintegrity.org/contracts/zpic-4
- Zone 5: nciinc.com/about-us/advancemed
- Zone 6: Not awarded at this time
- Zone 7: safeguard-servicesllc.com
- Eastern Benefit Integrity Support Center (EA-BISC) covers New York and New Jersey for Part A and B: safeguard-servicesllc.com/locations.asp
- New England Benefit Integrity Support Center (NEBISC) covers Medicare Part A including Home Health and Hospice and Part B in Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, Rhode Island and Vermont: safeguard-servicesllc.com/locations.asp#ne
- NEBISC covers Home Health and Hospice in New Jersey, New York and Pennsylvania: safeguard-servicesllc.com/locations.asp#ne
- NEBISC covers only Part B in the County of Fairfax, the County of Arlington and the City of Alexandria in Virginia: safeguard-servicesllc.com/locations.asp#ne
- Pennsylvania Benefit Integrity Support Center (PENN-BISC) covers Pennsylvania for Part A and B: safeguard-servicesllc.com/locations.asp#penn
- DME PSCs for Jurisdiction A: tricenturion.com/

- Medicare Part D Recovery Audit Contractor: cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/recovery-audit-program-parts-c-and-d/Part-D-Recovery-Audit-Contractor.html

Additional Resources

- Office of Inspector General (OIG) Compliance: https://oig.hhs.gov/compliance/
- OIG Fraud: https://oig.hhs.gov/fraud/
- OIG Corporate Integrity Agreements: https://oig.hhs.gov/compliance/corporate-integrity-agreements/index.asp
- FBI: fbi.gov/about-us/investigate/white_collar/health-care-fraud
- DEA: justice.gov/dea
- Stop Medicare Fraud: stopmedicarefraud.gov/index.html
- OIG database of excluded individuals/entities: https://oig.hhs.gov/exclusions/index.asp
- Excluded Parties List System (EPLS) on System for Award Management (SAM) website: https://www.sam.gov/portal/public/SAM

Public Information Resources

- Yellow Pages: yellowpages.com
- White Pages: whitepages.com
- AnyWho: anywho.com
- 411: 411.com

7.4.2. Interview Guide

Based on the information gathered during your preliminary investigation, you may determine an interview is helpful. Not every investigation benefits from an interview, and in some cases, it might be better not to conduct an interview. For example, if a criminal investigation is already underway, law enforcement might request that you not conduct interviews.

When an interview is appropriate, it gives you a chance to gather information from individuals with direct or indirect knowledge of an allegation. You might receive information about timelines, events, people involved, how the scheme evolved.

Once you have determined that an interview will help your investigation, you will want to decide whom to interview as well as where and how to conduct the interview.

Whom to Interview

As you conduct your investigation, there are several categories of interviewees who can provide valuable information:

- Subject of investigation
- Complainant(s), including enrollees
- Other contacts obtained through the interview/investigation process

As you conduct the interviews, it is a best practice to explore identified relationships from one interview to another.

Acquiring Additional Information without an Interview

If you decide not to conduct an interview you might still find additional documentation from a provider or any other subject of an investigation helpful to verify billed items/services, analyze claims information, or review compliance. You can consider sending a request for records to the provider via fax or mail. The Example Medical Records Request Letter provides an example of the type of letter that you might send to a provider to request records. Additional examples of records to request can be found in the Example Specialty Records Request Lists. If you choose to use the example letter or list, you may customize the content to meet the specific circumstances of your investigation and other needs of your organization.

Where and How to Conduct the Interview

You may decide to conduct the interview in person or over the phone. There are advantages and disadvantages to each, which you will need to consider.

In-Person Interviews. In-person interviews might occur in your office or in the home or office of the interviewee. Interviewing at the person's home or office provides the following advantages:

- You can view documents and leave with copies (e.g., professional or medical licenses).
- You are able to observe physical items (e.g., appropriate office equipment and space, equipment inventory).
- You can tour the office and/or facility to make sure they have equipment necessary to bill specific tests/labs, DME, or other services.
- You can observe the enrollee in his or her home and see if and how they use medical equipment (e.g., confirm equipment serial number, enrollee's level of activity).
- The interviewee is more comfortable in his or her own space and may be able to provide more information.

Some interviewees might prefer to come to your office so that others do not know they are being interviewed. Although you will lose the advantages listed above, the HCAA notes that there are some benefits to the interviewee coming to your office:

- You may have more control of the interview.
- There will be fewer distractions for the interviewee.
- The interviewee will realize how serious the situation is.
- The interviewee may speak more freely in the privacy of your office.

Phone Interviews. A phone interview might be on the only available way to interview an individual if he or she is not located within the area you are able to travel.

Telephone interviews have the following advantages:

- They are good for gathering initial information.
- You are able to get immediate information and insight.
- Interviewees might speak more freely over the phone.

However, HCAA also identifies disadvantages to phone interviews:

- You cannot observe the interviewee's body language.
- There is no eye contact.

Phone Interview Tips

- Listen intently to the interviewee
- Call from a quiet place such as a conference room or office

While conducting the interview, you may need to ask follow-up questions so it is important that you are able to hear clearly and remain focused on the conversation. If you want to record the interview, make sure you get the interviewee's permission on tape before you start. When possible, it is best to get this permission in writing from both parties in advance of the call. Also, have your interview questions prepared before the interview.

Preparing for the Interview

It is best practice to do as much background research on the interviewee and the allegation as you can before the interview. You will want to fully understand the interviewee's relationship to the allegation. Your focus during the interview should be on getting information/facts you did not already have and determining a direction for potential violations. Good sources of information might include (see Section 7.3. for additional documentation examples):

- Background information (e.g., past convictions or complaints)
- Billing information (e.g., data analysis of the subject's last three years of billing)
- Business information (e.g., professional or business licenses)
- Enrollment information (e.g., initial provider enrollment file and subsequent information obtained)
- Other available documents (e.g., EFT or EDI information)
- Internet searches (e.g., Secretary of State information)

It is also helpful to determine if the provider has any of the following types of information within your sponsor:

- Active or prior fraud grievances or complaints
- Active or prior referral to the CMS NBI MEDIC
- Prior overpayments or voluntary refunds and why
- Prior provider education provided by the sponsor

It is also good to review the provider enrollment file(s), including background check information for a complete view of the provider's business.

Your research will help you develop questions that you will ask to get the information you need. Open ended questions that require the interviewee to respond with information rather than a "yes" or "no" are best. In developing questions, remember to tailor them based on the level of understanding you can expect from the interviewee.

Below are some example question sets you might find helpful for interviewing (to access each of the forms, click on the links below or access the Appendix). If you choose to use these examples as a starting point for planning your interview questions, keep in mind that you can customize these examples to meet the specific circumstances of your investigation and other needs of your organization. As appropriate, you may add, delete, or re-order the example questions, and you may also reformat the examples according to your organization's document standards.

- Physicians or Non-Physician Practitioners
- Home Health Certifying Providers, DME Referring Providers, and Specialty DME Providers
- Pharmacy Providers

- Durable Medical Equipment Prosthetics, Orthotics and Supplies (DMEPOS) Providers
- Enrollees

Although there are times when an interview may be scheduled in advance, it can be advantageous to arrive at the interview location (e.g., provider's office or enrollee's home) and announce the interview at that time.

Conducting the Interview

It is a best practice to have at least two investigators participate in every interview, whether in person or over the phone. In this way, one interviewer to lead the interview which could include introductions, asking the interview questions and handling interviewee concerns. The second investigator could focus on taking notes to accurately record interviewee responses, including body language and other observations as well as take photographs as appropriate. It is recommended that the investigators agree to their respective roles prior to beginning the interview.

If you are conducting the interview at the interviewee's office or home, it is helpful to take a few minutes to assess the location before you enter the building or before beginning the interview. Information that you observe and record about things such as staffing, signage, and accessibility can be helpful as your investigation continues or if law enforcement accepts the case. The Example Pre-Interview/Site Visit Assessment demonstrates the type of information you might find helpful to record. (To access this form, click on the link or access the Appendix.) If you choose to use this example assessment form, remember that you can customize the form by adding or deleting information based on the needs of your investigation. You may also decide to reformat this example to complement other forms used within your organization.

Understand that the interviewee may be anxious and the way you conduct the interview can make the interviewee more comfortable and more willing to share information. It is important to be professional, and it is recommended that you begin the interview by identifying yourself and your organization and by explaining the purpose of the interview. If possible, you might provide a business card with your contact information. You might also consider providing a letter of introduction that explains the purpose of the interview. Below are links to several example letters that you may choose to use to introduce an interview or site visit. (To access each of the forms, click on the links below or access the Appendix.) If you choose to use these example letters, you may customize the content to meet the specific circumstances of your investigation and other needs of your organization.

- Example Non-Physician Site Visit Letter
- Example Enrollee Interview Introduction Letter

Interviewing Tips

Keep the following tips in mind as you begin the interview:

- Be firm but polite
- Do not alienate the interviewee by being aggressive or intimidating
- Use terminology that relates to the topic
- Use language that is easy to understand and appropriate to the interviewee
- Listen carefully
- Use good eye contact

Additionally, you may find it helpful to bring individual billing or prescribing data handouts with you. These could prove to be important information that the provider is unaware of. Examples of individual billing or prescribing data handouts could include summaries of past billing or referring provider history from your sponsor's claims system or data warehouse. These handouts could include information such as total billed and paid amounts with a claims count, top-billed items/services, or top referral sources. These handouts are helpful for planning the interview and may become a discussion point during the interview, if necessary.

Responding to Questions from Providers during the Interview. Providers may have some questions about the interview process. While it is important to provide honest responses to these questions, at the same time you need to maintain control of the interview situation. Anticipating questions and having answers prepared are helpful techniques for maintaining this authority.

The following are examples of provider questions during a site visit with example responses:

1. What is this about?
    - Response: We are here to discuss your Part C and/or Part D billing or orders/referrals based on a review of your billing over the last **[state time frame under investigation].**
    - Or: We are here to discuss a complaint regarding your Part C and/or Part D billing practices to **[state sponsor name**].
2. Do I need an attorney?
    - Response: If you feel you need one, please call one. We will wait. **[You should discuss how you would handle this question with your legal counsel/compliance team prior to a site visit. Also, be prepared to return at another time if the provider demands or requests to have an attorney present.]**

If it appears the provider has been a victim of identity theft, the provider may ask the following types of questions with the following example responses:

3. How can I protect myself?
    - Response 1: Allow the sponsor permission to install edits to deny claims for [**(state specific enrollee(s) or billing code(s)**] that you do not order or provide.
    - Response 2: Consider termination of your reassignment of benefits to the group practice.
4. What are you doing to protect my billing information?
    - For this question, it is best to develop your response by reviewing your organization's background check processes, and any ongoing enrollment checks your enrollment team performs.

Requesting Documents during the Interview. At the beginning of the interview or site visit, consider asking the provider to show you the originals of all requested documents. This can save you time by having the records copied while you are conducting the interview. If there are two or more interviewers

from the sponsor based on best practices, it is a good idea that one interviewer watch as the files are being copied to make sure no tampering of files is occurring.

It is best to leave with as many files as possible, but if the provider asks to fax or ship files at a later time, you may ask to see the originals (for later comparison to the copies) but attempt to leave with a percentage (such as 20%) of the requested records in your possession. Ask the interviewee to commit to sending copies of any remaining requested items by secure fax or registered/certified mail by a certain date. If the provider is sending copies and you have brought a camera, it is good to photograph the documents in the file to compare when the copies are delivered; however, you will need to be cautious to protect PHI contained in the photos. If possible, you might consider taking a portable scanner or photocopier in case the provider does not have a photocopier on site. If the interviewee objects to your request for records or questions your authority to get these materials, you may remind the individual that according to his or her agreement with your sponsor and in compliance with applicable HIPAA regulations, he or she is permitted to disclose PHI to you without consent of the person to whom that information pertains.

It is a good practice to have the interviewee sign an attestation acknowledging that they have provided or will provide the requested documents. The Example Access to Information Form demonstrates the type of statement that you might ask a provider to sign whether you leave with copies or the provider intends to send them by an agreed upon date. (To access this form, click on the link or access the Appendix.) If you choose to use this form, you may customize the content to meet the specific circumstances of your investigation and other needs of your organization. Additionally, you may reformat the document according to the communication standards of your organization.

Asking Questions during the Interview. The interview is an opportunity to get additional contacts and ask for additional information (e.g., DEA certificate, business license, mailers, medical license, equipment maintenance logs, inventory sheets, brochures, advertisement information, treatment protocols, agreements with vendors, subcontracts). If you get additional information, consider identifying and logging the items.

As you ask questions, it is best to take detailed notes about the interviewee's response and/or reaction (e.g. body language, eye contact). Also, you might keep the following guidelines in mind as you ask your questions:

- Ask general questions to understand how the interviewee operates or how a situation happened.
- Ask one question at a time.
- Ask questions in a logical order. Try to ask the questions as if in a conversation. It is okay to veer from your question order if that is how the conversation is flowing.
- Make sure each question is fully answered. Restate portions of a question if necessary to get a complete answer or to get additional information.
- Let the interviewee give you as much information as they are willing to share. Give the interviewee time to elaborate and provide as much detail as possible. Silence will often elicit additional information.

Concluding the Interview and Post Interview Activities

Before ending the interview you may want to recap the discussion to ensure that you recorded responses correctly and do not need additional information at this time. You might also remind the interviewee of any requested documents or records.

In instances of possible provider identity theft, the interview may conclude with the physician or other provider agreeing to corrective actions to protect his or her identity and prevent his or her billing number from being misused in the future with your sponsor.

- If the provider states he or she did not bill or order/refer the items and/or services for the enrollee(s) that you have shown him or her, it is recommended that you ask if he/she is willing to provide a signed attestation that will prevent his or her billing number from being misused in the future with your sponsor. It is also recommended that you get permission for an auto-denial edit for the provider for billing and/or ordering/referring with his or her provider number having the physician complete and sign a Physician Attestation. Note: even if the physician does not want edits put in place, it is advised that you ask him or her to sign the attestation and indicate this in the additional narrative section.
- If the physician indicates that he or she is allowing others to use his or her provider number, best practices indicate that you should ask if he or she would agree to terminate this risky behavior and have him or her complete and sign the Physician Attestation.
- If it appears that others in the group practice may be using the physician's number to bill without his or her knowledge, it is recommended that you ask if the physician would agree to voluntarily terminate his or her reassignment of benefits to the group practice and have him or her complete and sign the Physician Attestation.

The Example Provider Attestation Form can be used to document the corrective actions or you may choose to develop a similar document specifically for your sponsor. (To access this form, click on the link or access the Appendix.) If you choose to use this form, you may customize the content to meet the specific circumstances of your investigation and other needs of your organization. Additionally, you may reformat the document according to the communication standards of your organization.

Before leaving, it is best to ask for follow-up contact information in case you need more information or need to clarify what you have already discussed. It is also recommended that you retain originals of any documents the interviewee signed during the interview, leaving only copies.

Immediately following the interview, you might find it helpful to record at a high level the results of your interview and your general impressions. The Example Post-Provider Interview Results Form provides an example of the type of information that you might want to record after the interview. (To access this form, click on the link or access the Appendix.) If you choose to use this example worksheet as a starting point, remember that you may customize the content by adding or deleting items to meet the specific circumstances of your investigation and other needs of your organization. Additionally, you may reformat the document according to the communication standards of your organization. It is also best to type up your interview notes as soon as possible while the interview is still clear in your mind so that you do not forget any details.

7.5. HEAT Team and Strike Forces

The Health Care Fraud Prevention and Enforcement Action Team (HEAT) is an interagency task force of top-level law enforcement agents, prosecutors, and staff from the DOJ and HHS. HEAT investigates individuals or healthcare companies suspected of Medicare or Medicaid FWA.

The HEAT's mission is detailed on the Stop Medicare Fraud website (stopmedicarefraud.gov/heattaskforce/index.html). The mission information is listed below:

- To gather resources across government to help prevent FWA in the Medicare and Medicaid programs, and crack down on the fraud perpetrators who are abusing the system and costing us all billions of dollars
- To reduce skyrocketing healthcare costs and improve the quality of care by ridding the system of perpetrators who are preying on Medicare and Medicaid beneficiaries
- To highlight best practices by providers and public-sector employees who are dedicated to ending FWA in Medicare
- To build upon existing partnerships between DOJ and HHS, such as our Medicare Fraud Strike Forces, to reduce fraud and recover taxpayer dollars

The Medicare Fraud Strike Force is a multi-agency team of federal, state, and local investigators that operate in key cities and may use data analysis techniques to fight Medicare FWA. Medicare Strike Force teams are usually led by a federal prosecutor from the U. S. Attorney's Office, an FBI agent, and an HHS OIG agent.

The Medicare Fraud Strike Force's actions are detailed on the Stop Medicare Fraud website as:

- Expansion of the DOJ, CMS, and HHS Inspector General's Medicare Fraud Strike Forces to Baton Rouge, Brooklyn, Detroit, Houston, Los Angeles, Miami-Dade, Tampa Bay, Dallas, and Chicago.
- Use of new state-of-the-art technology to fight fraud. Investigators in the HHS Office of Inspector General are implementing state-of-the-art, cutting-edge technology to identify and analyze potential fraud with unprecedented speed and efficiency.
- Commitment to expanded data sharing and improved information sharing procedures between HHS and DOJ to get critical data and information into the hands of law enforcement to track patterns of FWA.
- President's 2010 budget for HHS contains funding for anti-fraud efforts covering a five-year period that is estimated to save $2.7 billion by improving overall oversight and stopping FWA within the Part C and Medicare Part D programs. It also invests $311 million to strengthen Medicare and Medicaid program integrity.
- Outreach meetings with top anti-fraud leaders in Congress, law enforcement, healthcare, and the private sector.

- New funding for and expanded use of Medicare Drug Integrity Contractors to monitor Part C and Part D compliance and enforcement.
- Expansion of the CMS Demonstration project on DME.
- Expansion of the CMS Medicaid provider audit program.
- Increased compliance training for providers.

Due to the fast pace and the focus of the HEAT and Medicare Fraud Strike Force, you may be directly contacted by one of the teams to request claims, enrollment, or other types of information to support an ongoing law enforcement investigation. The teams also work directly with the CMS NBI MEDIC through the RFI process.

8. REFERRAL

Making referrals — for any potential criminal, civil, or administrative law violation — is crucial to supporting CMS's efforts to track and fight Part C and Part D fraud nationally. When fraud perpetrators find a successful fraud model, they often use it on multiple private and federal healthcare organizations and programs in multiple locations. Some design "hit-and-run" fraud schemes that bleed sponsors out of millions of dollars in a few days and then quickly shut down and move somewhere else. Making referrals helps prevent identified fraud schemes from moving around the country and their perpetrators from being able to switch with impunity to new schemes in new locations.

This chapter provides information on the process for making referrals to the CMS NBI MEDIC and other law enforcement agencies such as the HHS OIG; considerations for making other criminal, civil, administrative, and state-level referrals; and resources that may be helpful in referring cases.

8.1. CMS NBI MEDIC Referrals

The CMS NBI MEDIC investigates Part C and Part D FWA cases involving sponsors, pharmacies, providers, or enrollees. The CMS NBI MEDIC is funded to refer Part C and Part D FWA investigations to law enforcement through the proper law enforcement channels.

After you make a referral to the CMS NBI MEDIC, it will conduct additional investigations and will refer to HHS OIG, the FBI, and state or local law enforcement, as appropriate. The CMS NBI MEDIC will also provide investigative support to your organization, the OIG, and law enforcement toward the prosecution and conviction of fraud perpetrators.

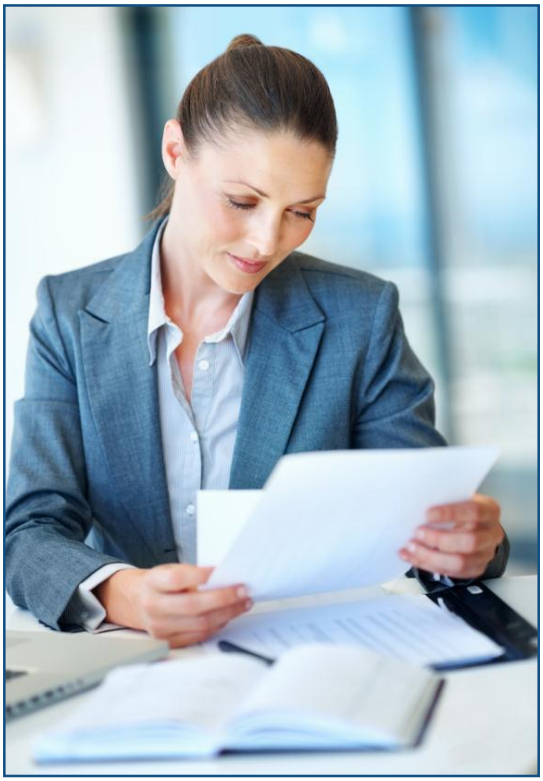
Referring investigations to the CMS NBI MEDIC is critical to helping CMS fight fraud nationwide. Besides coordinating with local, state, and federal law enforcement, the CMS NBI MEDIC uses data analytics to develop fraud scheme models to track fraud nationally. When you report to the CMS NBI MEDIC any potential fraud you identify in your network, CMS NBI MEDIC is

Combining Cases

Fraud perpetrators often spread their fraud scheme across multiple private and federal healthcare organizations and programs. Not only does this decrease the chance of detection, in the absence of information-sharing and coordination, it can lower the chance of prosecution. If the CMS NBI MEDIC can combine several sponsor investigations, a stronger case with a higher dollar threshold can be created that is more likely to result in successful prosecution.

able to incorporate the potential fraud that you detected into its fraud scheme models and reduce the time it takes to prevent, detect, and mitigate these schemes elsewhere in the country.

8.1.1. Timelines and Follow-Up



If the facts developed during your preliminary investigation lead you to believe a criminal, civil, or administrative law was violated, the matter should be referred promptly to the CMS NBI MEDIC and/or law enforcement. You can send a referral and continue with your investigation. If you continue with your investigation after the referral, notify the CMS NBI MEDIC and/or law enforcement in the event that you get additional information or want to take additional action such as a site visit. The CMS NBI MEDIC or law enforcement may ask that you not take any further action once law enforcement takes the case so as not to inadvertently interfere with a law enforcement investigation.

Be aware that it is the sponsor's responsibility to turn the investigation over to the CMS NBI MEDIC within 30 days if you do not have the time or resources to investigate, per the Compliance Program Guidelines.

The CMS NBI MEDIC will keep you apprised of the referral development and the status of the investigation, per the Compliance Program Guidelines. After you make a referral to the CMS NBI MEDIC, you will receive:

- An acknowledgment letter within five days of referral
- A resolution letter after the CMS NBI MEDIC's resolution action
- Status updates as requested; updates will be very high level and may be just that the investigation is open/active

Some cases may take years to be fully resolved and prosecuted. In some cases, such as the ones that go to trial, the CMS NBI MEDIC may request additional information from you or ask you to provide subject matter experts.

8.1.2. What to Refer to the CMS NBI MEDIC

Refer to the CMS NBI MEDIC anything meeting the following criteria:

- Potential criminal, civil, or administrative law violations
- Allegations including and extending beyond Part C and Part D, involving multiple sponsors, multiple states, or widespread schemes
- Allegations involving known patterns of fraud
- Patterns of fraud or abuse threatening the life or well-being of Part C and Part D enrollees

8.1.3. Information to Include in Referrals

You need to include enough specifics in your CMS NBI MEDIC and/or law enforcement referrals to allow an investigator to follow up:

- Your name, organization, and contact information
- Contact information for the suspected perpetrators
- Summary of the issue: the basic who, what, where, why, when, and how.
- The criminal, civil, or administrative laws (at the state or federal level) if you think there is probable cause to believe they were violated
- A detailed description of the allegations or fraud pattern to support why you think there is probable cause to believe criminal, civil, or administrative laws were violated
- List of incidents and issues related to the allegations
- Additional background information that may assist investigators, such as names and contact information of informants and witnesses, websites, geographic locations, corporate relationships, networks
- Perspective of your sponsor, CMS, and enrollees
- Supporting data, such as existing and potential data sources, graphs, and trends interview summaries, maps, and dollars at risk
- Any other referrals you have already made or administrative actions you have already taken (see Sections 8.2.2. and 8.2.3.)
- Recommendations for pursuing the investigation, including next steps, special considerations, and cautions

8.1.4. CMS NBI MEDIC Referral Process

Because information in the CMS NBI MEDIC referrals often includes data protected by HIPAA or the Privacy Act, only use one of the following two methods to make CMS NBI MEDIC referrals:

- Complete the CMS NBI MEDIC Complaint Form available online at healthintegrity.org/docs/NBI_Contract_HI_MEDIC_Complaint_Form_20111109.pdf. To report identity theft, use the CMS NBI MEDIC Compromised ID Report Form available online at: healthintegrity.org/docs/HI_MEDIC_Compromised_ID_Report_Form_20120515.pdf. Fax the forms to the CMS NBI MEDIC at (410) 819-8698 or mail them to:

  Health Integrity, LLC
  9240 Centreville Road
  Easton, MD 21601
  Attn.: CMS NBI MEDIC

- Call the CMS NBI MEDIC at 877-7SafeRX (877-772-3379) and provide the information to its complaint specialists who will key the information into a database and acknowledge and follow up on the complaint.

Identity Theft Reporting

If you want to report that the identity of a beneficiary, prescriber/provider, or pharmacy has been compromised, please complete and fax a Compromised ID Report Form available at healthintegrity.org/docs/HI_MEDIC_Compromised_ID_Report_Form_20120515.pdf to (410) 819-8698.

8.1.5. What You Can Expect from the CMS NBI MEDIC

Making referrals to the CMS NBI MEDIC offers several important benefits:

- **Investigative support**: The CMS NBI MEDIC's team of experienced Part C and Part D fraud investigators will handle the entire investigation. Your investigation will then benefit from combined cases, information in federal databases, invoice audit support, and coordination with law enforcement as detailed in the following bullets.
  - **Combined cases**: If the CMS NBI MEDIC can combine several sponsor investigations involving the same perpetrator, it increases the overall dollars at risk and documents widespread fraud — building a stronger case. Combining cases leads to more potential for law enforcement intervention.
  - **Access to information from federal databases**: When you make a referral to the CMS NBI MEDIC, your investigation will benefit from information in several federal databases that can build a stronger case. Examples of these databases are:

- **Federal Investigative Database (FID)** is a CMS database containing information on investigations CMS Program Safeguard Contractor (PSC) and Zone Program Integrity Contractor (ZPIC) Benefit Integrity (BI) units have investigated as well as cases that have been referred to law enforcement. The FID also captures information on payment suspensions that have been imposed. Through the FID, the CMS NBI MEDIC can determine whether law enforcement, PSC, or ZPIC BI units have already investigated an entity and entered relevant information about it.
- **Compromised Number Database** tracks compromised Medicare physician and sponsor member identification numbers. Numbers are identified through data analysis, fraud investigations, reports of security breaches, and enrollee or physician complaints.
- **Integrated Data Repository (IDR)** serves as a centralized and single repository that houses all Medicare claims, enrollee and provider enrollment data, and all PDE data.
- **One PI** is a portal with two analytical tools that the CMS NBI MEDIC can use to access and analyze IDR data.
- **STARS National Database** contains data relating to Medicare Part A, Part B, and Part C and can generate leads from Part D data.
- **Medicare Beneficiary Enrollment Database (MBD)** houses Medicare beneficiary and enrollment information provided by CMS.
- **Monthly Full Enrollment File Data (FEFD)** contains monthly enrollment data provided by CMS.

- **Invoice audit support**: The CMS NBI MEDIC's access to nationwide PDE data can provide invaluable support to your invoice audits. For example, if you get pharmacy invoices, the CMS NBI MEDIC can match the invoices to the nationwide PDE data to identify shortages between what the pharmacy billed and what it purchased. To verify the legitimacy of the drugs billed by the pharmacy, the sponsor may also request a drug manufacturer pedigree. A drug pedigree is a statement of origin that identifies each prior sale, purchase, or trade of a drug, including the date of those transactions and the names and addresses of all parties to them. You can then do an audit to determine what is left on site.
- **Coordination with law enforcement**: The CMS NBI MEDIC team will determine whether anyone else is already investigating the suspected fraud perpetrators and work with law enforcement and prosecutors to combine your referral into a larger case if appropriate. When the CMS NBI MEDIC does this coordination on your behalf, you save the time of having to report to different entities separately. Also, because the CMS NBI MEDIC works continually with law enforcement and prosecutors and has built strong working relationships, the CMS NBI MEDIC is positioned to identify and address issues early in investigations and build strong cases that are prosecuted successfully.

- **Resolution**: The CMS NBI MEDIC team will notify you of the resolution of your referral once actions are completed and the information is available.

8.1.6. What the CMS NBI MEDIC (and Federal Prosecutors) Will Expect from You

Whether your investigative staff or the CMS NBI MEDIC conducts your fraud investigations and/or coordinates with law enforcement, such as HHS OIG, you may be expected to provide subject matter experts and documentation to support a case.

Subject Matter Experts. As your case progresses, you may be asked to provide subject matter experts. Testimony and opinions from your subject matter experts may be kept confidential as part of attorney work products (i.e., documents attorneys use when working on a case and that are not shared with the other side) or may be entered into evidence during a trial. You need to take great care in choosing your subject matter experts to be prepared for either scenario. Besides choosing professionals who are the top in their field, it is critical to ensure your subject matter experts possess a high standard of honesty, integrity, and credibility.

Under Giglio v. United States,1972, investigative agencies must turn over to prosecutors, as early as possible in a case, potential impeachment evidence that might call into question or impeach the credibility of witnesses. This evidence includes, but is not strictly limited to:

- Specific instances of conduct of a witness for the purpose of attacking his or her credibility or character for truthfulness
- Evidence in the form of opinion or reputation as to a witness's character for truthfulness
- Prior inconsistent statements
- Information that may be used to suggest that a witness is biased

Prosecutors then exercise their discretion as to whether the impeachment evidence must be turned over to the defense. A "Giglio-impaired" witness is one against whom there is potential impeachment evidence that would render the witness's testimony of marginal value, potentially harming the case.

The best way to avoid having a Giglio-impaired witness derail a case is to:

- Take great care in the selection of subject matter experts
- Be honest and upfront about any misconduct
- Turn over any potential impeachment information to prosecutors as soon as you find out about it

Meticulous Chain of Custody (Physical Security and Packaging). After a referral, each investigation needs to be treated as if it will be prosecuted — with case files prepared and maintained assuming an appeal or federal court level of review. Thus, you need to have comprehensive and detailed case documentation, complete detailed description of activities, accurate and complete interview notes, and extensive contact information. It is critical that your investigative staff ensures the integrity of all evidence (e.g., its physical security and its admissibility and usefulness in legal proceedings) by properly documenting, handling, storing, and preserving it. This means taking steps from the moment you possess a given piece of evidence to establish its chain of custody:

- Documenting when and from where the evidence was received as well as from whom, and by whom.
- Tracking its handling from collection through its safeguarding, analysis, and introduction in legal proceedings. This includes documenting each person who handles the piece of evidence, the date/time of any transfers, and the reason for handling or transferring the evidence.

Keeping organized files will also help your investigative staff with any information requests from the CMS NBI MEDIC, which often have 30-day turnaround time frames (see the Compliance Program Guidelines). Be sure to respond to CMS NBI MEDIC and/or law enforcement requests with working copies of original documents and recordings, then store all original items — including investigators' original interview notes — in sealed containers in a secure location. Each original piece of evidence must be labeled with the identity of the person who handled it, the reason they handled it, the date, and the time. If the case goes to trial, originals with a solid chain of custody may be required.

Records Retention. Per federal regulations, Medicare Part C and Part D sponsors must retain records, files, and/or documents for at least 10 years and provide them to CMS on request. For fraud cases, however, a best practice is to retain related files indefinitely, because you may be asked by law enforcement to provider records, files, and/or documents related to cases years after the initial investigation began to support trial activity.

8.1.7. CMS NBI MEDIC-Returned Referrals

The CMS NBI MEDIC may elect to return your referral to you without further development or action. In such cases the CMS NBI MEDIC may advise you to take actions on your own. These actions can include the following:

- Notifying law enforcement, such as the HHS OIG, FBI, DEA, local police, directly
- Taking civil action to seek damages (see Section 8.2.1.)
- Making an administrative referral to a state department of insurance or licensing board (see Section 8.2.2.)
- Taking internal administrative actions (see Section 8.2.3.), such as subjecting the suspected fraud perpetrators to pre-payment review (see Section 6.2.) and data analytics (see Section 5.1.2.) — enabling you to update the dollars at risk, assess whether fraudulent activity is potentially continuing, and determine next steps for your investigation

8.2. Other Referrals and Actions

Whether or not you make a referral to the CMS NBI MEDIC or another law enforcement agency, you are free to take civil and administrative actions on your own or in conjunction with a referral. This section provides more detail on these actions.

8.2.1. Civil Action

Your organization may wish to pursue civil suits against FDRs who commit fraud, especially in cases with large financial exposure or dollars at risk. It is often best to pursue civil action after a criminal case is complete unless the prosecutor has no objection to a civil and criminal case occurring simultaneously. The U.S. Attorneys' Offices can be reluctant to initiate a criminal case if a civil case is already under way, and they may decline a case where a sponsor has already been made whole though civil action. Also, in some scenarios, where the evidence does not meet the standard of beyond a reasonable doubt for a criminal conviction but still may be sufficient to prove by a preponderance of the evidence for a civil judgment, the HHS OIG or FBI will seek civil monetary penalties. For these reasons, sponsors are discouraged from taking civil action until the CMS NBI MEDIC has taken a case up the law enforcement channels and law enforcement and prosecutors have reached a decision. To avoid jeopardizing cases, the best course of action is to contact the CMS NBI MEDIC and your CMS account manager for guidance before taking civil action.

8.2.2. Administrative Referral to State Regulatory Authorities

Your fraud investigation may determine that a fraud perpetrator's improper conduct could affect his or her license or certification. In these scenarios, you should refer the matter to the proper licensing entity for administrative action. These entities include state departments of insurance (e.g., to sanction fraudulent marketing agents) or state boards that license medical professionals (e.g., doctors, nurses, therapists). State regulations may require you make these administrative referrals within a certain time period. It is important that you follow all state regulations and reporting requirements thoroughly.

Some state regulatory authorities report their Part C and Part D criminal investigations to CMS regional offices, which, in turn, report them to the CMS NBI MEDIC. While the CMS NBI MEDIC does not routinely make referrals to state regulatory authorities, however, they may request that you refer an investigation to a state entity and that you inform them of the referral. This information assists the CMS NBI MEDIC's staff with tracking fraud patterns nationally.

8.2.3. Internal Administrative Action

There are three main scenarios for taking internal administrative action.

- **Suspension and termination:** You may decide an FDR's conduct was improper enough to warrant suspending or terminating the FDR from your organization.
- **Negotiated settlement**: Your fraud investigation may identify monies improperly paid to an FDR, but the evidence does not support moving forward with a civil or criminal case. Consider contacting the FDR to negotiate a settlement based on the identified over-payment amount.
- **Prepayment review and data analytics:** Other internal administrative actions to take include subjecting the prescriber/provider to pre-payment review (see Section 6.2.) and using data analytics (see Section 5.1.2.) to monitor all enrollees, prescribers/providers, or pharmacies associated with the suspected fraud scheme.

The CMS NBI MEDIC would like to be informed of any administrative actions you take against FDRs.

8.3. Resources

This section provides additional referral resources.

8.3.1. CMS

- CMS NBI MEDIC Compromised ID Report Form: healthintegrity.org/docs/HI_MEDIC_Compromised_ID_Report_Form_20120515.pdf
- CMS NBI MEDIC Complaint Form: healthintegrity.org/docs/NBI_Contract_HI_MEDIC_Complaint_Form_20111109.pdf

8.3.2. Other Federal Agencies

- DEA Office of Diversion Control website: deadiversion.usdoj.gov
- FBI healthcare fraud webpage: fbi.gov/about-us/investigate/white_collar/health-care-fraud
- HHS OIG report fraud webpage: https://oig.hhs.gov/fraud/report-fraud/index.asp

8.3.3. Associations

- American Medical Association links to state medical boards: ama-assn.org/ama/pub/education-careers/becoming-physician/medical-licensure/state-medical-boards.page
- Association of State and Provincial Psychology Boards' contact information for state and territorial agencies responsible for the licensure and certification of psychologists throughout the United States: http://www.asppb.net/?page=BdContactNewPG
- Federation of State Medical Boards directory of state medical and osteopathic boards: fsmb.org/directory_smb.html
- National Association of Board of Pharmacy state boards of pharmacy contact information: nabp.net/boards-of-pharmacy

APPENDIX

Abbreviations Used

AC — Affiliated Contractor

ACFE — Association of Certified Fraud Examiners

AoA — Administration on Aging

BISC — Benefit Integrity Support Center

CEO — Chief Executive Officer

CFR — Code of Federal Regulations

CIA — Corporate Integrity Agreement

CMHC — Community Mental Health Center

CMP — Civil Monetary Penalties

CMS — Centers for Medicare & Medicaid Services

CMS NBI MEDIC — National Benefit Integrity MEDIC

CMS O&E MEDIC — Outreach and Education MEDIC

CNC — Compromised Number Contractor

COB — Coordination of Benefits

CTM — Complaint Tracking Module

DEA — Drug Enforcement Administration

DHS — Designated Health Service

DMAC — Durable Medical Equipment Medicare Administrative Contractor

DME — Durable Medical Equipment

DMEPOS — Durable Medical Equipment Prosthetics Orthotics and Supplies

DOJ — Department of Justice

DSB — Drug Seeking Beneficiaries

DUR — Drug Utilization Review

E & M — Evaluation and Management

EA-BISC — Eastern Benefit Integrity Support Center

EDI — Electronic Data Interchange

EFT — Electronic Funds Transfer

EIN — Employer Identification Number

EKG — Electrocardiogram

EPLS — Excluded Parties List System

FAKS — Anti-Kickback Statute

FBI — Federal Bureau of Investigation

FFCA — False Claims Act

FDA — Food and Drug Administration

FDR — First-Tier, Downstream, and Related Entities

FEFD — Full Enrollment File Data

FID — Federal Investigative Database

FWA — Fraud, Waste, and Abuse

GAO — Government Accountability Office

GSA — General Services Administration

HCCA — Health Care Compliance Association

HCPCS — Healthcare Common Procedure Coding System

HEAT — Health Enforcement Action Team

HEDIS — Health Plan Employer Data and Information Set

HHS — Health and Human Services

HICN — Health Insurance Claim Number

HIPAA — Health Insurance Portability and Accountability Act

HIPDB — Health Integrity and Protection Database

HPMS — Health Plan Management System

HRA — High-Risk Area

IASIU — International Association of Special Investigative Units

IDR — Integrated Data Repository

LEIE — List of Excluded Individuals/Entities

MA — Part C

MAC — Medicare Administrative Contractor

MAO — Part C Organization

MAPD — Part C Prescription Drug Plan

MBD — Medicare Beneficiary Database

MD — Medical Doctor

MEDIC — Medicare Drug Integrity Contractor

MFCU — Medicaid Fraud Control Units

MIPPA — Medicare Improvements for Patients and Providers Act

MMCM — Medicare Managed Care Manual

MMDRF — Medicare Master Death Records File

NCBOE — National Center for Benefits Outreach and Enrollment

NCD — National Coverage Determination

NCPDP — National Council for Prescription Drug Programs

NEBISC — New England Benefit Integrity Support Center

NHCAA — National Health Care Anti-Fraud Association

NPI — National Provider Identifier

OASIS — Outcome & Assessment Information Set

OIG — Office of Inspector General

One PI — One Program Integrity

P&T — Pharmacy & Therapeutic

PA — Prior Authorization

PACER — Public Access to Court Electronic Records

Part C — Medicare Part C Program

Part D — Medicare Prescription Drug Program

PBM — Pharmacy Benefit Managers

PDE — Prescription Drug Event

PDBM — Prescription Drug Manual

PDP — Prescription Drug Plan

PHI — Protected Health Information

PIM — Program Integrity Manual

PSC — Program Safeguard Contractor

PT — Physical Therapist

QIO — Quality Improvement Organization

RAC — Recovery Audit Contractor

RFI — Request for Information

RN — Registered Nurse

SDP — Self Disclosure Protocol

SHIP — Senior Health Information Assistance Program

SIU — Special Investigations Unit

SMP — Senior Medicare Patrol

STARS — Services Tracking Analysis and Reporting System

UPIN — Unique Physician Identification Number

USC — United States Code

USPS — United States Postal Service

ZPIC — Zone Program Integrity Contractor

Websites and Resources

Affordable Care Act: housedocs.house.gov/energycommerce/ppacacon.pdf

Anti-Kickback Statute (AKS): gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap7-subchapXI-partA-sec1320a-7b.pdf

Association of Certified Fraud Examiners (ACFE): acfe.com

CMS NBI MEDIC Complaint Form: healthintegrity.org/docs/NBI_Contract_HI_MEDIC_Complaint_Form_20111109.pdf

False Claims Act: gpo.gov/fdsys/pkg/USCODE-2010-title31/pdf/USCODE-2010-title31-subtitleIII-chap37-subchapIII-sec3729.pdf

Health Care Compliance Association (HCCA): hcca-info.org

Health Information Portability and Accountability Act Resources: hhs.gov/ocr/privacy/hipaa/understanding/index.html

International Association of Special Investigative Units (IASIU): iasiu.org

National Benefit Integrity (NBI) MEDIC Case Referral: healthintegrity.org/contracts/nbi-medic/referring-fraud-waste-or-abuse-cases

National Center for Benefits Outreach and Enrollment (NCBOE): ncoa.org/enhance-economic-security/center-for-benefits/

National Health Care Anti-Fraud Association (NHCAA): nhcaa.org.

National State Health Insurance Assistance Program (SHIP) Website: shiptalk.org/default.aspx?ReturnUrl=%2f

Outreach & Education (O&E) MEDIC Website: medic-outreach.rainmakerssolutions.com

Senior Medicare Patrol (SMP) National Resource Center: smpresource.org

Stark Law: gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap7-subchapXVIII-partE-sec1395nn.pdf

US Attorney's Office Directory: usdoj.gov

Contacts

CMS National Benefit Integrity (NBI) MEDIC

- If you suspect Part C or Part D fraud, waste, or abuse, please contact the CMS NBI MEDIC at 1-877-7SAFERX (1-877-772-3379). If you have questions for the CMS NBI MEDIC, please see the list of CMS NBI MEDIC contacts at healthintegrity.org/contact-us/nbi-medic-contacts.

CMS Outreach and Education (O&E) MEDIC

- For information about Medicare Parts C and D Fraud Work Group meetings, educational activities, conference participation or this website, please contact MEDIC-Outreach@rainmakerssolutions.com.

Division of Plan Oversight & Accountability (DPOA)

- DPOA is part of the Center for Program Integrity within CMS. If you have comments or questions for CMS, please email DPOACommunications@cms.hhs.gov.

CMS/HHS Contacts

Links below take you to a directory for each CMS Regional Office, including contact information for regional director, chief council, special agent in charge, and others.

Region	States Served	Contacts Page
One	CT, MA, ME, NH, RI, VT	www.hhs.gov/about/regions/r1contacts.html
Two	NJ, NY, PR	www.hhs.gov/about/regions/r2contacts.html
Three	DC, DE, MD, PA, VA, WV	www.hhs.gov/about/regions/r3contacts.html
Four	AL, FL,GA, KY, MS, NC, SC,TN	www.hhs.gov/about/regions/r4contacts.html
Five	IL, IN, MI, MN,OH, WI	www.hhs.gov/about/regions/r5contacts.html
Six	AR, LA, NM, OK, TX	www.hhs.gov/about/regions/r6contacts.html
Seven	IA, KS,MO, NE	www.hhs.gov/about/regions/r7contacts.html
Eight	CO, MT, ND, SD, UT, WY	www.hhs.gov/about/regions/r8contacts.html
Nine	AZ, CA, HI, NV	www.hhs.gov/about/regions/r9contacts.html
Ten	AK, ID, OR, WA	www.hhs.gov/about/regions/r10contacts.html

DOJ (U.S. Attorneys' Offices) by State

State	District	Offices	Website
Alabama	Northern	Birmingham, Huntsville	www.justice.gov/usao/aln
	Middle	Montgomery, Opelika, Dothan	www.justice.gov/usao/alm
	Southern	Mobile	www.justice.gov/usao/als
Alaska	-	Anchorage, Juneau, Fairbanks	www.justice.gov/usao/ak
Arizona	-	Phoenix, Flagstaff, Yuma, Tucson	www.justice.gov/usao/az
Arkansas	Eastern	Little Rock	www.justice.gov/usao/are
	Western	Fort Smith	www.justice.gov/usao/arw
California	Northern	San Francisco, Oakland, San Jose	www.justice.gov/usao/can
	Central	Los Angeles, Santa Ana, Riverside	www.justice.gov/usao/cac
	Eastern	Sacramento, Fresno	www.justice.gov/usao/cae
	Southern	San Diego, Imperial	www.justice.gov/usao/cas
Colorado	-	Denver, Durango, Grand Junction	www.justice.gov/usao/co
Connecticut	-	New Haven, Bridgeport, Hartford	www.justice.gov/usao/ct
Delaware	-	Wilmington	www.justice.gov/usao/de
District of Columbia	-	Washington, D.C.	www.justice.gov/usao/dc
Florida	Middle	Tampa, Jacksonville, Fort Meyers, Ocala, Orlando	www.justice.gov/usao/flm
	Northern	Tallahassee, Gainesville, Panama City, Pensacola	www.justice.gov/usao/fln
	Southern	Miami	www.justice.gov/usao/fls
Georgia	Middle	Macon, Albany, Columbus	www.justice.gov/usao/gam
	Northern	Atlanta	www.justice.gov/usao/gan
	Southern	Savannah, Augusta	www.justice.gov/usao/gas
Guam & Northern Mariana Islands	-	Hagåtña, Saipan	www.justice.gov/usao/gu
Hawaii	-	Honolulu	www.justice.gov/usao/hi
Idaho	-	Boise, Coeur d'Alene, Pocatello	www.justice.gov/usao/id
Illinois	Central	Springfield, Peoria, Rock Island, Urbana	www.justice.gov/usao/ilc
	Northern	Chicago, Rockford	www.justice.gov/usao/iln
	Southern	Fairview Heights, Benton	www.justice.gov/usao/ils
Indiana	Northern	Hammond, Fort Wayne, South Bend	www.justice.gov/usao/inn
	Southern	Indianapolis, Evansville	www.justice.gov/usao/ins

State	District	Offices	Website
Iowa	Northern	Cedar Rapids, Sioux City	www.justice.gov/usao/ian
	Southern	Des Moines, Davenport, Council Bluffs	www.justice.gov/usao/ias
Kansas	-	Wichita, Kansas City, Topeka	www.justice.gov/usao/ks
Kentucky	Eastern	Lexington, Ft. Mitchell, London	www.justice.gov/usao/kye
	Western	Louisville, Paducah, Bowling Green, Owensboro	www.justice.gov/usao/kyw
Louisiana	Eastern	New Orleans	www.justice.gov/usao/lae
	Middle	Baton Rouge	www.justice.gov/usao/lam
	Western	Shreveport, Lafayette	www.justice.gov/usao/law
Maine	-	Portland, Bangor	www.justice.gov/usao/me
Maryland	-	Baltimore, Greenbelt	www.justice.gov/usao/md
Massachusetts	-	Boston, Springfield, Worcester	www.justice.gov/usao/ma
Michigan	Eastern	Detroit, Bay City, Flint	www.justice.gov/usao/mie
	Western	Grand Rapids, Marquette, Lansing	www.justice.gov/usao/miw
Minnesota	-	Minneapolis, St. Paul	www.justice.gov/usao/mn
Mississippi	Northern	Oxford	www.justice.gov/usao/msn
	Southern	Jackson, Gulfport	www.justice.gov/usao/mss
Missouri	Eastern	St. Louis, Cape Girardeau	www.justice.gov/usao/moe
	Western	Kansas City, Jefferson City, Springfield	www.justice.gov/usao/mow
Montana	-	Billings, Butte, Great Falls, Helena, Missoula	www.justice.gov/usao/mt
Nebraska	-	Omaha, Lincoln	www.justice.gov/usao/ne
Nevada	-	Las Vegas, Reno	www.justice.gov/usao/nv
New Hampshire	-	Concord	www.justice.gov/usao/nh
New Jersey	-	Newark, Camden, Trenton	www.justice.gov/usao/nj
New Mexico	-	Albuquerque, Las Cruces	www.justice.gov/usao/nm
New York	Eastern	Brooklyn, Central Islip	www.justice.gov/usao/nye
	Northern	Albany, Syracuse, Binghamton, Plattsburgh	www.justice.gov/usao/nyn
	Western	Buffalo, Rochester	www.justice.gov/usao/nyw
	Southern	Boroughs of Manhattan and Bronx; counties of Dutchess, Orange, Putnam, Rockland, Sullivan, and Westchester	www.justice.gov/usao/nys

State	District	Offices	Website
North Carolina	Eastern	Raleigh	www.justice.gov/usao/nce
	Middle	Greensboro, Winston-Salem	www.justice.gov/usao/ncm
	Western	Charlotte, Asheville	www.justice.gov/usao/ncw
North Dakota	-	Fargo, Bismarck	www.justice.gov/usao/nd
Ohio	Northern	Cleveland, Akron, Toledo, Youngstown	www.justice.gov/usao/ohn
	Southern	Columbus, Dayton, Cincinnati	www.justice.gov/usao/ohs
Oklahoma	Eastern	Muskogee	www.justice.gov/usao/oke
	Northern	Tulsa	www.justice.gov/usao/okn
	Western	Oklahoma City	www.justice.gov/usao/okw
Oregon	-	Portland, Eugene, Medford	www.justice.gov/usao/or
Pennsylvania	Eastern	Philadelphia	www.justice.gov/usao/pae
	Middle	Harrisburg, Scranton, Williamsport	www.justice.gov/usao/pam
	Western	Pittsburgh, Erie, Johnstown	www.justice.gov/usao/paw
Puerto Rico	-	San Juan	www.justice.gov/usao/pr
Rhode Island	-	Providence	www.justice.gov/usao/ri
South Carolina	-	Columbia, Charleston, Florence, Greenville	www.justice.gov/usao/sc
South Dakota	-	Sioux Falls, Pierre, Rapid City, Aberdeen	www.justice.gov/usao/sd
Tennessee	Eastern	Knoxville, Chattanooga, Greenville, Johnson City	www.justice.gov/usao/tne
	Middle	Nashville, Columbia, Cookeville	www.justice.gov/usao/tnm
	Western	Memphis, Jackson	www.justice.gov/usao/tnw
Texas	Eastern	Beaumont, Lufkin, Sherman, Tyler, Plano, Texarkana	www.justice.gov/usao/txe
	Northern	Dallas, Amarillo, Ft. Worth, Lubbock	www.justice.gov/usao/txn
	Southern	Houston, Brownsville, Corpus Christi, Laredo, McAllen, Victoria	www.justice.gov/usao/txs
	Western	San Antonio, Alpine, Austin, Del Rio, El Paso, Midland, Pecos, Waco	www.justice.gov/usao/txw
Utah	-	Salt Lake City	www.justice.gov/usao/ut
Vermont	-	Burlington, Rutland	www.justice.gov/usao/vt
Virgin Islands	-	St. Thomas, St. Croix	www.justice.gov/usao/vi
Virginia	Eastern	Alexandria, Norfolk, Richmond, Newport News	www.justice.gov/usao/vae
	Western	Roanoke, Abingdon, Charlottesville	www.justice.gov/usao/vaw

State	District	Offices	Website
Washington	Eastern	Spokane, Yakima	www.justice.gov/usao/wae
	Western	Seattle, Tacoma	www.justice.gov/usao/waw
West Virginia	Northern	Wheeling, Clarksburg, Elkins, Martinsburg	www.justice.gov/usao/wvn
	Southern	Charleston, Huntington	www.justice.gov/usao/wvs
Wisconsin	Eastern	Milwaukee	www.justice.gov/usao/wie
	Western	Madison	www.justice.gov/usao/wiw
Wyoming	-	Cheyenne, Casper, Lander, Yellowstone National Park	www.justice.gov/usao/wy

Job Aids and Techniques for Investigation Development

This section corresponds to the Interview Guide in Section 7.4.2. It includes a variety of job aids available in the Appendix such as example letters, interview question sets, forms, and worksheets that you may find helpful in developing your investigation. If you choose to use these job aids, you can use them as published or tailor them to the specific needs of your organization.

Example Medical Records Request Letter

If you choose to use the following example medical records request letter, customize the letter with the appropriate content for your organization and the specific circumstances of the investigation. The [highlighted prompts] are intended to assist you with this customization. You may also choose to add or delete language as necessary to reflect your organization's contractual relationship/agreement with providers. ***Delete the green instructions.***

Date

Provider Name

Provider Address

City, State ZIP

Re: Medical Records Request for Provider [Sponsor Identifier Number/NPI]

Dear Provider:

[Name of Sponsor] is reviewing claims billed by you or containing your provider identifier billing number and/or National Provider Identifier (NPI) as the [supplying/ordering/referring provider]. This comprehensive review of your billing for services is pursuant to your contractual agreement with [Name of the Sponsor]. You were selected for this review because our analysis of your billing data indicates that you may be [rationale statement such as: billing inappropriately for services].

The following example text can be used for a SVRS record request. Delete this language if you are not using a SVRS.
We have selected a statistically valid random sample of [total number of claims in the sample] claims for services provided from [initial date of service or receipt date] through [last date of service or receipt date]. (Please see attached listing. ***Attach a listing of claims from your sample.***) For each of these claim(s), we are requesting the following information:

The following example text can be used for a non-random sample record request. Delete this language if you are not using a non-random sample.
We have selected a total of [total number of claims in the review] claims for services provided from [initial date of service or receipt date] through [last date of service or receipt date]. (Please see attached listing. ***Attach a listing of claims from your sample.***) For each of these claim(s), we are requesting the following information:

Insert a list of documents requested for the claims. See the Example Specialty Records Request Lists for suggested documentation pertaining to:

- ***Inpatient***
- ***Skilled Nursing***
- ***Mental Health***
- ***Home Health***
- ***Durable Medical Equipment (DME)***
- ***Pharmacy***

As appropriate for your investigation, you may use the example lists as provided or modify the lists by adding or deleting items. You may also choose to develop your own lists for these specialties or other specialties not listed.

Also, please include the following documents related to your business, which could include but are not limited to the following documents:

The following is an example business document list. You can tailor this list to the provider or specialty and to the needs of your organization. You may also choose to remove this section if it is not relevant.

- Proof of accreditation
- All appropriate licensure and certification applicable to your classification
- Fire Department Inspection Certification (if applicable)
- Comprehensive liability insurance
- List of current and former sales representatives (names/SSNs/contact information)
- List of current and former employees (names/SSNs/contact information)
- Proof of enrollee co-payment (if applicable)

As a healthcare provider, you are a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) if you (or a third party acting on your behalf, such as a billing service) electronically transmit health information in connection with claims, benefit eligibility inquiries, referral authorization requests, or other transactions. As part of your agreement with [Name of Sponsor] and in compliance with applicable HIPAA regulations, you are permitted to disclose protected health information to [Name of Sponsor] without consent of the person to whom that information pertains.

We appreciate your cooperation regarding this matter. If you have any questions, you may call our office at [Sponsor phone number].

Sincerely,

[Sponsor Representative Name]

Enclosure: Listing of Claims Requiring Medical Documentation (For HIPAA compliance consider including only the enrollee's last name, last four digits of his/her HICN.)

Example Specialty Records Request Lists

Supplement to Example Medical Records Request Letter

SPECIALTY RECORDS REQUEST LISTS

Example Inpatient Record Request

(Suggested documents for proof of need or requirement of services. Not to be considered an inclusive or a required list of records.)

- Physician orders
- Prior authorization number (if applicable)
- Physician progress notes
- Nursing progress notes
- History and physical
- Admission notes
- Discharge notes
- Procedure/operative notes
- Laboratory results
- Medication administrative records
- Social services notes
- Therapy evaluation(s), plan(s) of care and progress notes (if applicable)
- All transfer records
- Case management notes
- Enrollee notice of liability
- Authorization of benefits
- Consent for treatment
- All other documentation to support billed services

Example Skilled Nursing Facility (SNF) Record Request

(Suggested documents for proof of need or requirement of services. Not to be considered an inclusive or a required list of records.)

- History and physical or hospital discharge summary
- Facility admission notes
- Facility history and physical
- Physician orders
- Physician progress notes
- Nursing progress notes
- Prior authorization (if applicable)
- All plans of care
- Occupational, physical, and speech therapy evaluations
- Occupational, physical, and speech therapy notes
- Occupational, physical, and speech therapy recertification(s)
- Occupational, physical, and speech therapy discharges summaries
- Occupational, physical, and speech therapy minutes/logs
- Medication record or medication administration records, including any IV medications
- Laboratory/test results performed while in SNF
- Facility discharge summary
- Skin and wound care notes
- Respiratory and oxygen records
- Assessment information
- Certification/recertification forms
- All documentation supporting the patient's need for and delivery of the skilled service provided

Example Mental Health Record Request

(Suggested documents for proof of need or requirement of services. Not to be considered an inclusive or a required list of records.)

SPECIALTY RECORDS REQUEST LISTS

- Physician orders
- Physician certification/recertification(s) orders
- Current individualized, multi-disciplinary treatment plan to include updates/revisions to the plan of care
- Initial psychiatric assessment
- Prior authorization (if applicable)
- Psychiatric progress notes
- Psychological testing reports/results
- Psychological initial intake
- Physician progress notes
- Nursing progress notes
- All daily individual and group therapy notes
- Admission notes
- Discharge notes
- History and physical
- Laboratory results
- Medication orders
- Patient roster
- Certificate of medical necessity
- Authorization of benefits
- Consent for treatment
- All other documentation necessary to support the billed service(s)

Example Home Health/Hospice Records Request

(Suggested documents for proof of need or requirement of services. Not to be considered an inclusive or a required list of records.)

- All assessment information forms completed during the period under review (ex. admission, recertification)
- Documentation justifying the medical necessity of services
- Signed physician plan of care/certification/recertification orders
- Signed supplemental orders or telephone orders
- History and physical
- Hospital discharge summary (if applicable)
- Admission notes
- Discharge notes
- Nursing progress notes
- Therapy (physical, occupational and/or speech therapy) evaluation(s), plan(s) of care and notes
- Home health aide notes
- Social worker notes
- Supervisor visits
- Laboratory results
- Medication sheets
- Patient roster
- Documents or photographs identifying the enrollee
- Consent for treatment
- Assignments of benefits authorization (signed by enrollee)
- All other documentation to support billed services

Example Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) Supplier Records Request

SPECIALTY RECORDS REQUEST LISTS

(Suggested documents for proof of need or requirement of services. Not to be considered an inclusive or a required list of records.)

- Signed prescriptions or orders for the item and all accessories
- Any documentation in the file justifying the medical necessity of the DMEPOS
- Manufacturer's brochure pertaining to the DMEPOS provided to the enrollee
- Purchasing invoices pertaining to the DMEPOS provided to the enrollee
- Dated and signed proof of delivery receipts
- Assignment of benefits authorization (signed by enrollee)
- Pick-up receipts showing returned items by the enrollee (if applicable)
- Documents or photographs identifying the enrollee

Example Pharmacy Records Request

(Suggested documents for proof of need or requirement of services. Not to be considered an inclusive or a required list of records.)

- Signed prescriptions/orders or telephone orders
- Signed required pharmaceutical form(s), if applicable
- Any documentation in the file justifying the medical necessity of the medication
- Dated and signed documentation that the enrollee received the medication

Example Interview Questions

Physicians or Non-Physician Practitioners

If you choose to use these example interview questions for physicians or non-physician practitioners customize the following form with the appropriate content for your organization and the specific circumstances of the interview/investigation. The [highlighted prompts] are intended to assist you with this customization. You may also choose to add or delete questions as necessary.

INTERVIEW QUESTIONS FOR PHYSICIANS OR NON-PHYSICIAN PRACTITIONERS				
Physician or Practitioner Information				
Provider Name:		Sponsor Billing Identifier Number:		
Provider Telephone Number:		NPI Number:		
Provider Specialty:		Other Related Numbers or NPIs:		
Office Address:		Other Office Locations:		
Source of Identification Verification, e.g., license, passport (record number):				
Interview Information				
Interviewers:				
Date:	Start Time:	End Time:	Language:	Location:

General Questions	
1.	In what state(s) do you have an active medical license?
2.	What is your specialty? Any additional specialties?
3.	What is your primary location? How long have you been practicing there? What are your days and hours of operation?
4.	Have you practiced in any other state within the past five years? If so, where and when?
5.	Are you part of a group practice? If so, what is the group information?
6.	When and how did you join this group? (e.g., Internet ad, newspaper) (*Discuss business relationship for each practice location*)
7.	Do you use a billing firm/agency to submit your claims to the sponsor? If so, what is its name, address, phone number, and manager's name? (*Request a copy of the signed contract*)
8.	What percentage of your billing is to [Name of Sponsor] for Part C and/or Part D? What are other insurance companies you bill? (*Request the approximate percentage for each entity*)
9.	What are your approximate Part C and/or Part D earnings?
10.	Do you supervise Physician's Assistants? If so, what are their names? What are their NPIs? Do you bill the sponsor for their services? Are they allowed to prescribe medications, medical supplies and equipment, and home health services? Can they admit patients to the hospital? Can they order labs or other services?
11.	Do you supervise Nurse Practitioners? If so, what are their names? What are their NPIs? Do you bill the sponsor for their services? Are they allowed to prescribe medications, medical supplies and equipment, and home health services? Can they admit patients to the hospital? Can they order labs or other services?
12.	Did you ever give anyone permission or authority to use your sponsor billing identifier number? If so, whom?

INTERVIEW QUESTIONS FOR PHYSICIANS OR NON-PHYSICIAN PRACTITIONERS	
13.	Do you have an office management group working for you? If so, please provide the name, address, and telephone number. What is the manager's name and contact information? Who is the owner of the practice, and what is his or her contact information? (*Request a copy of the signed contractual arrangement*)
14.	How do you get paid by the sponsor (e.g., electronic fund transfer, check)? If you have a bank account, does anyone else have access to it, and are you the only signatory? (*If multiple locations or group practices, ask questions for each location*)
15.	How do you obtain your patient base (e.g., walk-ins or referrals)? If referrals, who refers patients to you?
16.	Have you ever treated and rendered medical services to these patients? (*Consider presenting the provider with a listing of enrollees for which the provider has billed or ordered items and/or services. This can be obtained from your claims data. Have physician/practitioner check off names of all his/her patients.*)

Home Health Certifying Providers, DME Referring Providers, and Specialty DME Providers

If you choose to use these example interview questions, select the appropriate group of example questions and customize them with appropriate content for your organization and the specific circumstances of the interview/investigation. You may also choose to add or delete questions as necessary.

INTERVIEW QUESTIONS FOR HOME HEALTH CERTIFYING PROVIDERS, DME REFERRING PROVIDERS, AND SPECIALTY DMEPOS REFERRING PROVIDERS	
Example Interview Questions for Home Health Certifying Provider	
1.	Do you prescribe home health/physical therapy/diagnostic testing for your Part C patients? a. If yes, did you prescribe these services for any of the enrollees that you identified on the list as being your patients? *(This list can be obtained from your claims data of Home Health Agency [HHA] services billed.)* b. If you prescribe home healthcare, are you an employee of the home health agency? If so, what are your approximate annual earnings in this capacity? *(If the physician is part of a group practice, consider asking if anyone in the group would have prescribed home healthcare for his/her patients.)*
2.	How do you evaluate and determine an enrollee/patient is home-bound or home confined?
3.	How do you develop a plan of care?
Example Interview Questions for DME Referring Provider	
1.	Do you prescribe durable medical equipment for your Part C patients? a. If so, what types? b. Please estimate the types/number of units of equipment/supplies that you have prescribed for your Part C patients. *(If the physician is part of a group practice, consider asking if anyone in the group would have prescribed equipment/supplies for his/her Part C patients.)*
2.	Is this/are these enrollee(s) your patient(s)? (*This list can be obtained from your claims data for DME services billed.)* a. Did you prescribe equipment/supplies for any of the enrollees that you identified on the list as being your Part C patients? b. If so, what types?

	(If the physician acknowledges having prescribed equipment/supplies to any/all of the patients on the list, consider asking him/her to provide you with the medical records for the enrollees. For patients for whom the doctor said he/she did not prescribe equipment/supplies, ask him/her to provide their medical records also.)
3.	Did you conduct a face-to-face examination/screening of the enrollee? If no, please explain who examined the enrollee.
4.	If so, do the medical records delineate the history of events that led to the request for the equipment/supplies that you prescribed?
5.	Does the medical record identify what equipment/supplies were ordered?
6.	Does the enrollee use the equipment/supplies?
7.	Does the medical record document the use of the equipment/supplies?
8.	Did you reorder the equipment/supplies? Does the medical record document this? *(This question would be important in the case of exhaustible supplies such as ostomy, catheter, or diabetic supplies since they are prospectively ordered or for a replacement piece of equipment.)*
9.	Describe who completed or filled out the physician's order and/or prescription for the equipment/supplies for the enrollee.
10.	Did the supplier or enrollee initiate the prescription/order for the equipment/supplies prior to you prescribing the equipment/supplies? If yes, explain.
11.	Do you receive any documents/faxes to sign for prescriptions/orders for equipment/supplies that you did not initiate? If yes, explain.
12.	What equipment/supplies provider(s), if any, do you normally conduct business with or suggest to your Part C patients?
13.	Are you familiar with the suppliers on this list that included you as the referral source on billed claims? a. If so, which ones? b. Did you prescribe equipment/supplies provided by them? *(Consider showing the physician the list of providers who have billed the sponsor for equipment/supplies he/she ordered.)*
Example Interview Questions for Specialty DME Referring Providers	
Oxygen Supplies and Equipment Questions	
1.	What types of oxygen supplies do you prescribe?
2.	Do you specialize in specific respiratory conditions?
3.	What are the diagnoses for the prescriptions/orders that you usually write for oxygen and oxygen supplies?
4.	Do you have an affiliation with a sleep study laboratory?
Wheelchair/Power Mobility Device (PMD) Questions	
1.	What types of wheelchairs or PMDs do you prescribe?
2.	Do you specialize in a specific area that includes rehab patients?
3.	What are the diagnoses for the prescriptions/orders that you usually write for PMDs?
4.	How do you establish what type of PMD is prescribed? a. Do you work with a physical therapist to determine the appropriate device? If so, what is the name of the therapist, phone, and address? b. Do you take into account whether the patient has the physical and mental abilities to transfer to a wheelchair/PMD and operate it safely?
Diabetic Supplies Questions	

1.	What type of diabetic equipment or supplies do you prescribe?
2.	What are the diagnoses for the prescriptions/orders that you usually write for diabetic supplies?
3.	What is the highest number of times per day you would instruct a Part C patient to test his/her blood: a. If they are insulin dependent? b. If they are non-insulin dependent?
4.	Do you or your staff consult with the patient before signing a new prescription/order for diabetic supplies?
Hospital Beds Questions	
1.	What type of hospital beds do you prescribe?
2.	How do you determine what type to prescribe?
3.	Do you have patients that require bariatric hospital beds?
Orthotics Questions	
1.	What type of orthotics do you prescribe? a. Do you prescribe prefabricated orthotics? b. Do you prescribe custom-fabricated or custom-made orthotics?
2.	Do you prescribe: a. Spinal orthotics? b. Elbow orthotics? c. Knee orthotics? d. Shoulder orthotics? e. Wrist, hand, finger orthotics? f. Any other types?
3.	How do you determine what type to prescribe? *(i.e., customized vs. prefabricated)*
4.	Do you fit the patient to the orthotic? a. If not, do you work with the supplier to fit the patient to the orthotic?
5.	Do you sign prescriptions/orders received by suppliers that you did not initiate?
Continuous Positive Airway Pressure (CPAP) Questions	
1.	How do you determine that a Part C patient needs a CPAP?
2.	Do you specialize in respiratory care?
3.	What type of sleep study do you prefer your Part C patients undergo*? (i.e., inpatient, sleep laboratory, home sleep study)*
4.	What are the diagnoses for the prescriptions/orders that you usually write CPAP and supplies?
5.	Are you affiliated with a sleep study laboratory?
6.	Do you or your staff consult with the Part C patient before signing a new prescription/order for CPAP supplies?
7.	Do you sign prescriptions/orders from suppliers for CPAP supplies only?
8.	Do you verify the patient has a CPAP before signing the prescription/order?

Pharmacy Providers

If you choose to use these example interview questions for pharmacy providers, customize the following form with the appropriate content for your organization and the specific circumstances of the interview/investigation. The [highlighted prompts] are intended to assist you with this customization. You may also choose to add or delete questions as necessary.

INTERVIEW QUESTIONS FOR PHARMACY PROVIDERS				
Pharmacy Provider Information				
Provider Name:			Sponsor Billing Identifier Number:	
Provider Telephone Number:			NPI Number:	
Office Address:			Other Related Numbers or NPIs:	
			Other Office Locations:	
Source of Identification Verification, e.g., license, passport (record number):				
Interview Information				
Interviewers:				
Date:	Start Time:	End Time:	Language:	Location:
General Questions				
1.	In what state(s) do you have an active pharmacy license? In the past five years?			
2.	What is the primary location? How many locations are there? How long has the business been located there? What are your days and hours of operation?			
3.	Who is the pharmacy owner and what is the contact information?			
4.	If you are not the pharmacy owner, when and how did you join this pharmacy? (e.g., Internet ad, newspaper)			
5.	Do you use a billing firm/agency to submit your claims to the sponsor? If so, what is its name, address, phone number, and manager's name? (*Request a copy of the signed contract*)			
6.	Did you ever give anyone permission or authority to use your sponsor billing identifier number? If so, whom?			
7.	What percentage of your billing is to [Name of Sponsor] for Part C and/or Part D enrollees? What are other insurance companies you bill? (*Request the approximate percentage for each entity*)			
8.	What are your approximate Part C and/or Part D earnings?			
9.	What is the breakdown of your staff? *(i.e., number of pharmacist, pharmacy technicians, billing analyst) (Request names, titles and contact information for present and past employees)*			
10.	How is a Part D enrollee referred to your pharmacy? *(e.g., walk-ins or referrals)* If referrals, who refers patients to you? *(Consider having a list of referring physicians with you so you can verify the names of the referring physicians the pharmacy provides to you. You can obtain this information from your claims data.)*			
11.	How do you receive prescriptions/orders for medications/supplies? *(i.e., faxed to you, given to you directly by the enrollee, do you pick them up from the physician?)*			
12.	How do you obtain your patient base)? If referrals, who refers patients to you?			
13.	Do you ever make contact with the referring physician(s) for the medications/supplies that you bill for? If so, explain.			

INTERVIEW QUESTIONS FOR PHARMACY PROVIDERS	
14.	How do you get paid by the sponsor (e.g., electronic fund transfer, check)? If you have a bank account, does anyone else have access to it, and are you the only signatory? (*If multiple locations ask questions for this information for each location*)
15.	What types of medications/supplies do you dispense? *(i.e., antibiotics, narcotics, ointments, TPN, enteral nutrition)*
16.	Have you ever filled prescriptions for these patients? (*Consider presenting the provider with a listing of enrollees for which this pharmacy provider has billed medications/supplies. This can be obtained from your claims data. Have the pharmacist or owner check off names of all his/her pharmacy patients on the list.*)

Durable Medical Equipment Prosthetics, Orthotics and Supplies (DMEPOS) Providers

If you choose to use these example interview questions for DMEPOS providers, customize the following form with the appropriate content for your organization and the specific circumstances of the interview/investigation. The [highlighted prompts] are intended to assist you with this customization. You may also choose to add or delete questions as necessary.

INTERVIEW QUESTIONS FOR DMEPOS PROVIDERS				
PROVIDER INFORMATION				
Provider Name:			Sponsor Billing Identifier Number:	
Provider Telephone Number:			NPI Number:	
Office Address:			Other Related Provider Numbers or NPIs:	
Other Facility Locations:				
INTERVIEWEE INFORMATION				
Name of Person Being Interviewed:			Job Title/Role:	
Source of Identification Verification, e.g., license, passport (record number):				
INTERVIEW INFORMATION				
Interviewers:				
Date:	Start Time:	End Time:	Language:	Location:
INTERVIEW QUESTIONS				
1.	Who owns the company? Please provide name, address, and phone number.			
2.	What is the primary location? How many locations are there? What are the days and hours of operation?			
3.	Do you use a billing firm/agency to submit your claims to the sponsor? If so, what is its name, address, phone number, and manager's name? (*Request a copy of the signed contract*)			
4.	What percentage of your billing is to [Name of organization] for Part C and/or Part D patients? (*Request the percentage approximate for each line of business*)			
5.	Who are you accredited by? (*Request a copy of the accreditation documentation*) If you are not yet accredited, are you planning to become so?			
6.	Do you have a surety bond? (*Request a copy of the surety bond*) If you do not, are you planning to acquire one?			

INTERVIEW QUESTIONS FOR DMEPOS PROVIDERS	
7.	What is the breakdown of your staff (e.g., medical director, number of billing analysts)? (*Request names, titles, and contact information of the present and past employees*)
8.	How are enrollees referred to your company?
9.	What equipment and/or supplies do you provide? (*If the supplier has a catalogue demonstrating the products, photocopy the appropriate pages. Additionally, take photos of the equipment in warehouse and showroom, as well as delivery vehicles if present. If no inventory is present take photos of empty space where you would expect these to be stored.*)
10.	How do you receive prescriptions/orders for the equipment and/or supplies you provide? *(i.e., are they faxed to you, given to you directly by the enrollees, and/or do you pick them up from the physician?)*
11.	How do you fill the prescription/order? Specifically, if a home visit and evaluation are required, who conducts them? (*Examples of delivery include: direct shipped, patient pick up, provider delivers to patient home. Ask provider to explain and show proof of delivery, e.g., shipping log/documents, patient signature on delivery ticket. Request copies of proof of delivery.*)
12.	Do you have any personal interaction with the referring physician(s) for the equipment and/or supplies for which you have billed? (*Show list of referring physicians to the supplier, which you can obtain from your claims data.*)

Enrollees

If you choose to use these example interview questions for enrollees, customize the following form with the appropriate content for your organization and the specific circumstances of the interview/investigation. The [highlighted prompts] are intended to assist you with this customization. You may also choose to add or delete questions as necessary.

INTERVIEW QUESTIONS FOR ENROLLEES				
ENROLLEE INFORMATION				
Enrollee Name:		Enrollee Number:		Date of Birth:
Home Address:		Telephone Number:		
INTERVIEWEE INFORMATION				
Person Interviewed if not Enrollee:		Relationship to Enrollee:		Contact Information:
INTERVIEW INFORMATION				
Interviewers:				
Date:	Start Time:	End Time:	Language:	Location:
INTERVIEW QUESTIONS				
1.	Are you covered by any other healthcare insurance besides [Name of Sponsor]?			
2.	What are your major medical problems or conditions? How long have you had them?			
3.	Do you have a primary care physician? Where is he/she located?			
4.	How often do you see this physician? When was the last time you saw him/her?			
5.	Are you under the care or treatment of other physicians or providers?			
6.	What services/items do you see each of them for?			
7.	Have you heard of [Provider name]? Were you ever treated by this provider? If not, have you heard of this provider?			

INTERVIEW QUESTIONS FOR ENROLLEES	
8.	Did you receive services from this provider on the following dates: [specific dates of service]? Describe the services.
9.	Did you have an examination by the provider?
10.	Who referred you to this provider? Were you approached by someone on the street or in a public place?
11.	How do you get to the provider's office? For example, your own car, public transportation, ambulance, other?
12.	Did you receive money or gifts to go to the provider's office? If so, please describe them.
13.	What equipment, supplies, and/or services (if any) have you been prescribed? Who prescribed them?
14.	What pharmacy or pharmacies do you use?
15.	What medications have you taken and what are the dosages?
16.	Are you using the equipment, supplies, and/or services prescribed? Can you show them to me (e.g., DME, diabetic supplies, prescription medication)? How long have you been using them? Where did you get them and what is the name of the provider that provided them?
17.	Have you ever lost your insurance card or given your sponsor number to anybody to use?
18.	If you have co-payments, who pays your co-payments?
19.	Do you receive Home Health Services? If so, what is the company's name and contact information (phone and address information)?
20.	How many times does the Home Health Agency (HHA) visit you per week? What are the names and phone numbers of the nurses that visit you?
21.	What do the nurses do when they visit?
22.	Do you receive any other services such as housekeepers, ambulance, adult day care? If so, what are the names and contact information of these providers?

Example Pre-Interview/Site Visit Assessment

If you choose to use this example assessment form, customize the following form with appropriate content for your organization and the specific circumstances of the interview/investigation. You may also choose to add or delete information as necessary.

PRE-INTERVIEW/SITE VISIT ASSESSMENT
1. When you arrive at the provider's location, determine which of the following applies: ☐ Does not exist ☐ Closed during posted business hours ☐ Closed and vacant ☐ Open and staffed ☐ Open but not staffed (e.g., provider is sharing space with another provider and there is no staff on site for the provider you are visiting) ☐ Unable to visually inspect to make a determination if the provider is open for business due to: ☐ Other, please describe:
2. Describe the physical location (appropriate site, signage, handicap accessibility, other business in close proximity, color of building (brick, wood), location of front and back doors). This description can be helpful to law enforcement.
3. Is there a visible sign with the provider's business name posted on the facility? ☐ Yes ☐ No If YES, provide the name of the company on the sign:
4. Are the hours of operation posted? ☐ Yes ☐ No If YES, list the hours of operation:
5. Is the facility staffed at the time of the site visit? If so, by whom?
6. Do the names on the door match the names on the provider's license?
7. Does the provider appear to be operating within his or her license, sponsor agreement?
8. Describe the provider's equipment and/or inventory that you were able to observe:
9. Other observations:

Example Non-Physician Site Visit Letter

If you choose to use this example letter for non-physician site visits, customize the following letter with the appropriate content for your organization and the specific circumstances of the interview/investigation. The [highlighted prompts] are intended to assist you with this customization. You may also choose to add or delete language as necessary to reflect your organization's contractual relationship/agreement with providers. ***Delete the green instructions.***

Additionally, you may choose to print the letter using your organization's letterhead and/or reformat the letter to meet the communication standards of your organization.

Provider Name: Sponsor Identifier Number:

Provider NPI:

Provider Address:

Provider Telephone Number:

Date of Provider Contact: Time of Provider Contact:

Provider Initials: _____

[Name of Sponsor] Representative Name:

Dear Provider:

[Name of Sponsor] is reviewing claims billed by you or containing your billing identifier number or National Provider Identifier (NPI) as the rendering provider. We would like to interview you about a list of enrollees as well as your overall business practices. The individuals presenting this letter to you are employees from [Name of Sponsor]. They have official identification credentials available for you to examine.

During this review, please understand that they may request access to information regarding your business and claims submitted for payment. As part of this review, they may request to review the originals and/or obtain copies of entire patient files of the enrollees on the list that will be provided to you, which could include but is not limited to the following documents. Please note that based on the results of this review, they may need to ask for additional information.

Insert a list of documents requested for the claims. See the Example Specialty Records Request Lists for suggested documentation pertaining to:

- ***Inpatient***
- ***Skilled Nursing***
- ***Mental Health***
- ***Home Health***
- ***Durable Medical Equipment (DME)***
- ***Pharmacy***

As appropriate for your investigation, you may use the example lists as provided or modify the lists by adding or deleting items. You may also choose to develop your own lists for these specialties or other specialties not listed.

The reviewers may also request to review documents related to your business.

As a healthcare provider, you are a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) if you (or a third party acting on your behalf, such as a billing service) electronically transmit health information in connection with claims, benefit eligibility inquiries, referral authorization requests, or other transactions. As part of your agreement with [Name of Sponsor] and in compliance with applicable HIPAA regulations, you are permitted to disclose protected health information to [Name of Sponsor] without consent of the person to whom that information pertains.

We appreciate your cooperation regarding this matter. If you have any questions, you may call our office at [Sponsor phone number].

Sincerely,

[Sponsor Representative Name]

Example Enrollee Interview Introduction Letter

If you choose to use this example letter as an introduction for enrollee interviews, customize the following letter with the appropriate content for your organization and the specific circumstances of the interview/investigation. The [highlighted prompts] are intended to assist you with this customization. You may also choose to add or delete language as necessary to reflect your organization's relationship with enrollees. ***Delete the green instructions.***

Additionally, you may choose to print the letter using your organization's letterhead and/or reformat the letter to meet the communication standards of your organization.

Dear [Enrollee's Name]:

[Name of Sponsor] periodically conducts reviews to ensure the quality and effectiveness of our enrolled providers. We are making home visits and/or telephone calls to conduct personal interviews with selected enrollees. The reason you are receiving this letter is because you have been selected to participate in a review.

Your interview responses are very important and will be combined with the responses of other enrollees like yourself. Please note that your participation in this review will not affect your coverage eligibility.

[Name of Sponsor] will protect the information you provide to the maximum extent permitted by law. We have long recognized the sensitivity of patient identifying information and take all appropriate physical and administrative safeguards to protect it from unauthorized use. Our office also adheres to confidentiality procedures regarding the provision and use of healthcare information in accordance with guidelines issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The individuals presenting this letter to you are employees from [Name of Sponsor]. They have official identification available for you to examine. ***Delete this paragraph if conducting a telephone interview.***

Thank you for your cooperation.

Sincerely,

[Sponsor Representative Name]

Example Access to Information Form

If you choose to use this example Access to Information form, customize the following form with the appropriate content for your organization and the specific circumstances of the interview/investigation. The [highlighted prompts] are intended to assist you with this customization. You may also choose to add or delete information as necessary.

ACCESS TO INFORMATION	
Provider Name:	Sponsor Billing Identifier Number: Provider NPI:
Provider Address:	Provider Telephone Number:
Date of Provider Contact:	Time of Provider Contact:
Provider Initials:	Sponsor Representative Name:
I, [Provider Name], certify that I have received a list of Part C and/or Part D enrollees from [Sponsor Name]. This list includes [total number of enrollees on list] enrollees. I have agreed to make copies of all medical records (including prescriptions and all other documents contained in patient file) for each of the [total number of enrollees on list] enrollees on this list. 1) ☐ I will make copies of the entire file, including any and all documentation that supports the billing for the attached list of enrollees, such as [document request list that is specific to the provider specialty or the billed items/services], and other information as specified below. OR 2) ☐ I will make copies of the entire file, including any and all documentation that supports the billing of the attached list of enrollees, such as [document request list that is specific to the provider specialty or the billed items/services] and other information as specified below. I agree to return the list and requested documents by [specific due date] to [specific Sponsor contact name] at [Sponsor contact information].	
Additional documentation requested:	
Signature of Provider: _____	Date of Provider Signature: _____

Example Provider Attestation Form

If you choose to use this example attestation form, customize the following form with the appropriate content for your organization and the specific circumstances of the interview/investigation. The [highlighted prompts] are intended to assist you with this customization. You may also choose to add or delete information as necessary.

PROVIDER ATTESTATION

In an effort to avoid the potential misuse of my sponsor identifier number and/or National Provider Identifier (NPI) by [Name of provider who is suspected of using the number without consent], I, [Provider name], wish to voluntarily give permission to [Name of Sponsor] to take appropriate actions based on this attestation, such as calculating an overpayment(s) and/or installing system edits preventing future payments. I attest that:

☐ **I have never billed** [items/services]**.** Any claim submitted with my sponsor identifier number and/or NPI for the above items/services would be an inappropriate use of my sponsor identifier number and/or NPI.

☐ **I have never ordered/referred** [items/services]**.** Any claim submitted by [Name of provider who is suspected of using the number without consent] with my sponsor identifier number and/or NPI as the ordering/referring physician would be an inappropriate use of my sponsor identifier number and/or NPI.

☐ **I have only ordered/referred** [items/services]. Any claim submitted by [Name of provider who is suspected of using the number without consent] with my sponsor identifier number and/or NPI as the ordering/referring provider for [items/services] other than the following items/services would be an inappropriate use of my sponsor identifier number and/or NPI.

Items/Services for which I have ordered:

I would like this statement to be effective immediately. Provider Initials: _____

I understand that if at any time I find it is necessary to amend this statement, I will contact [Name of Sponsor] to complete a new Physician Attestation to allow appropriate claims processing for services ordered/referred by me. Provider Initials: _____

I certify that I have thoroughly reviewed and understand all the information contained in this attestation. I also certify that this is a true and accurate attestation that I make freely and voluntarily and without any threats against me or promises to me. Provider Initials: _____

PROVIDER ATTESTATION		
Provider Information _____ *Signature* Name: Date: Time: Provider NPI: Sponsor Identifier Number: Mailing Address: Telephone number(s):	**Witness Information** _____ *Signature* Name: Title: Date: Time: Sponsor Representative Name: Contact number(s):	**Individual Providing Narrative Information:** _____ *Signature* Name: Date: Time:
This attestation was signed at (physical location/street address):		
Additional Narrative:		

Example Post-Provider Interview Results Form

If you choose to use this example form to record the results of your interview, customize the following form with the appropriate content for your organization and the specific circumstances of the interview/investigation. The [highlighted prompts] are intended to assist you with this customization. You may also choose to add or delete information as necessary.

POST-PROVIDER INTERVIEW RESULTS	
1. Does the provider order [Enter items/services]?	☐ Yes ☐ No
If YES, did he or she order all the [Enter items/services] billed on his or her behalf?	☐ Yes ☐ No
If NO, what types of [Enter items/services] did he or she order?	
What types of [Enter items/services] did he or she not order?	
2. Does the provider treat or see the patients on the list?	☐ All ☐ Some ☐ None
If SOME, how many did he/she treat or see?	
How many patients are on the list?	
3. Does the provider have medical records for all of the sample patients on the list?	☐ Yes ☐ No
If NO, how many does he have records for?	
4. Is the provider in active practice?	☐ Yes ☐ No
In how many states? Which states?	
5. Does the provider recognize or do business with any of the providers on the list?	☐ Yes ☐ No
If YES, how many?	
6. Does the provider appear to be the victim of identity theft?	☐ Yes ☐ No
7. Does the provider appear to be participating in the scheme?	☐ Yes ☐ No
8. Did the provider sign the attestation?	☐ Yes ☐ No
9. Did the provider agree to be placed on edit?	☐ Yes ☐ No
If YES, enter billing codes or other specific elements for included in the edit criteria. *Note: it is also recommend recording this information as part of a signed attestation by the provider.*	