CMS Manual System	Department of Health & Human Services (DHHS)
Pub 100-08 Medicare Program Integrity	Centers for Medicare & Medicaid Services (CMS)
Transmittal 176	Date: NOVEMBER 24, 2006
	Change Request 5368

SUBJECT: Various Benefit Integrity (BI) Revisions to Chapter 4

I. SUMMARY OF CHANGES: Various benefit integrity (BI) sections in chapter 4 of the PIM were revised to reflect updates and clarifications. Since the transition of all BI work to PSCs has been completed, all references to Medicare contractor BI unit were deleted. MAC responsibilities as they relate to BI and supporting PSCs have been added to chapter 4 of the PIM.

CLARIFICATION
EFFECTIVE DATE: December 26, 2006
IMPLEMENTATION DATE: December 26, 2006

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R=REVISED, N=NEW, D=DELETED

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
R	4/4.1/Introduction
R	4/4.2/The Medicare Fraud Program
R	4/4.2.1/Examples of Medicare Fraud
R	4/4.2.2/Program Safeguard Contractor Benefit Integrity Unit
R	4/4.2.2.1/Organizational Requirements
R	4/4.2.2.2/Liability of Program Safeguard Contractor Benefit Integrity Unit Employees
R	4/4.2.2.3/Anti-Fraud Training
R	4/4.2.2.3.1/Training for Law Enforcement Organizations
R	4/4.2.2.4.1/Maintain Controlled Filing System and Documentation
R	4/4.2.2.6/Benefit Integrity Security Requirements
R	4/4.2.3/Durable Medical Equipment Fraud Functions
R	4/4.3/Medical Review for Benefit Integrity Purposes
R	4/4.4.1/Requests for Information From Outside Organizations
R	4/4.4.1.1/Sharing Fraud Referrals Between the Office of Inspector

	General and the Department of Justice
R	4/4.4.2.1/Program Safeguard Contractor Coordination With Other Entities
R	4/4.4.3/Beneficiary, Provider, Outreach Activities
R	4/4.5/The ARGUS System
R	4/4.6.2/Complaint Screening
R	4/4.6.3/Filing Complaints
R	4/4.7/Investigations
R	4/4.7.1/Conducting Investigations
R	4/4.7.2/Closing Investigations
R	4/4.8/Disposition of Cases
R	4/4.8.1/Reversed Denials by Administrative Law Judges on Open Cases
R	4/4.9.1/Incentive Reward Program General Information
R	4/4.9.2/Information Eligible for Reward
R	4/4.9.3/Persons Eligible to Receive a Reward
R	4/4.9.4/Excluded Individuals
R	4/4.9.6/Program Safeguard Contractor Responsibilities
R	4/4.9.6.1/Guidelines for Processing Incoming Complaints
R	4/4.9.6.2/Guidelines for Incentive Reward Program Complaint Tracking
R	4/4.9.6.3/Overpayment Recovery
R	4/4.9.6.4/Eligibility Notification
R	4/4.9.6.5/Incentive Reward Payment
R	4/4.9.6.6/Reward Payment Audit Trail
R	4/4.9.7/CMS Incentive Reward Winframe Database
R	4/4.9.8/Updating the Incentive Reward Database
R	4/4.10/Fraud Alerts
R	4/4.10.1/Types of Fraud Alerts
R	4/4.10.2/Alert Specifications
R	4/4.10.3/Editorial Requirements
R	4/4.10.4/Coordination
R	4/4.10.5/Distribution of Alerts
R	4/4.11/Fraud Investigation Database Entries

R	4/4.11.1/Background
R	4/4.11.1.1/Information Not Captured in the FID
R	4/4.11.1.2/Entering OIG Immediate Advisements into the FID
R	4/4.11.2/Investigation, Case, and Suspension Entries
R	4/4.11.2.1/Initial Entry Requirements for Investigations
R	4/4.11.2.2/Initial Entry Requirements for Cases
R	4/4.11.2.3/Initial Entry Requirements for Payment Suspension
R	4/4.11.2.4/Update Requirements for Investigations
R	4/4.11.2.5/Update Requirements for Cases
R	4/4.11.2.7/OIG Non-Response to or Declination of Case Referral
R	4/4.11.2.8/Closing Investigations
R	4/4.11.2.9/Closing Cases
R	4/4.11.2.11/Duplicate Investigations, Cases, or Suspensions
R	4/4.11.2.12/Deleting Investigations, Cases, or Suspensions
R	4/4.11.3.1/Access
R	4/4.11.3.2/The Fraud Investigation Database User's Group
R	4/4.11.3.3/Designated PSC BI Unit Staff and the Fraud Investigation Database
R	4/4.11.3.4/The Fraud Investigation Database Mailbox
R	4/4.12.2/Harkin Grantee Tracking Instructions
R	4/4.12.3/System Access to Metaframe and Data Collection
R	4/4.12.4/Data Dissemination/Aggregate Report
R	4/4.13/Administrative Relief from Benefit Integrity Unit Review in the Presence of a Disaster
R	4/4.14/Provider Contacts by the Program Safeguard Contractor Benefit Integrity Unit
R	4/4.16/AC, MAC, and PSC Coordination on Volunatry Refunds
R	4/4.18.1/Referral of Cases to the Office of the Inspector General/Office of Investigations
R	4/4.18.1.2/Immediate Advisements to the OIG/OI
R	4/4.18.1.3/Program Safeguard Contractor BI Unit Actions When Cases Are Referred to and Accepted by the OIG/OI
R	4/4.18.1.3.1/Suspension
R	4/4.18.1.3.2/Denial of Payments for Cases Referred to and Accepted by OIG/OI

R	4/4.18.1.3.3/Recoupment of Overpayments
R	4/4.18.1.4/OIG/OI Case Summary and Referral
R	4/4.18.1.5.1/Continue to Monitor Provider and Document Case File
R	4/4.18.1.5.2/Take Administrative Action on Cases Referred to and Refused by OIG/OI
R	4/4.18.1.5.3/Refer to Other Law Enforcement Agencies
R	4/4.18.2/Referral to State Agencies or Other Organization
R	4/4.18.3/Referral to Quality Improvement Organizations
R	4/4.19/Administrative Sanctions
R	4/19.1/The Program Safeguard Contractor's Affiliated Contractor's and Medicare Administrative Contractor's Role
R	4/4.19.2/Authority to Exclude Practitioners, Providers, and Suppliers of Services
R	4/4.19.2.2/Identification of Potential Exclusion Cases
R	4/4.19.2.3/Development of Potential Exclusion Cases
R	4/4.19.2.4/Contents of Sanction Recommendation
R	4/4.19.2.6/Denial of Payment to an Excluded Party
R	4/4.19.2.6.1/Denial of Payment to Employer of Excluded Physician
R	4/4.19.2.6.2/Denial of Payment to Beneficiaries and Others
R	4/4.19.4/Reinstatements
R	4/4.19.4.1/Monthly Notification of Sanction Actions
R	4/4.20.1.2/Purpose
R	4/4.20.1.4/Administrative Actions
R	4/4.20.3.1/Referral Process to CMS
R	4/4.20.3.2/Referrals to OIG
R	4/4.20.4/CMS Generic Civil Monetary Penalties Case Contents
R	4/4.20.5.1/Beneficiary Right to Itemized Statement
R	4/4.20.5.2/Medicare Limiting Charge Violations
R	4/4.21/Monitor Compliance
R	4/4.21.1/Resumption of Payment to a Provider - Continued Surveillance After Detection of Fraud
R	4/4.22/Discounts, Rebates, and Other Reductions in Price
R	4/4.22.1.1/Marketing to Medicare Beneficiaries

R	4/4.22.2/Cost-Based Payment (Intermediary and Medicare Administrative Contractor Processing of Part A Claims): Necessary Factors for Protected Discounts
R	4/4.22.3/Charge-Based Payment (Intermediary and Medicare Administrative Contractor Processing of Part B Claims): Necessary Factors for Protected Discounts
R	4/4.23/Hospital Incentives
R	4/4.24/Breaches of Assignment Agreement by Physician or Other Supplier
R	4/4.25/Participation Agreement and Limiting Charge Violations
R	4/4.26/Supplier Proof of Delivery Documentation Requirements
R	4/4.26.1/Proof of Delivery and Delivery Methods
R	4/4.27/Annual Deceased-Beneficiary Postpayment Review
R	4/4.28/Joint Operating Agreement
R	4/4.31/Vulnerability Report
R	Exhibits/Table of Contents
R	Exhibit 37/Office of Inspector General, Office of Investigations Data Use Agreement

III. FUNDING:

No additional funding will be provided by CMS; contractor activities are to be carried out within their FY 2007 operating budgets.

IV. ATTACHMENTS:

Business Requirements
Manual Instruction

Unless otherwise specified, the effective date is the date of service.

Attachment - Business Requirements

Pub. 100-08	Transmittal: 176	Date: November 24, 2006	Change Request: 5368

SUBJECT: Various Benefit Integrity (BI) Revisions to Chapter 4

Effective Date: December 26, 2006

Implementation Date: December 26, 2006

I. GENERAL INFORMATION

A. Background: Various benefit integrity (BI) sections in chapter 4 of the PIM were revised to reflect updates and clarifications. Since the transition of all BI work to PSCs has been completed, all references to Medicare contractor BI unit were deleted. MAC responsibilities as they relate to BI and supporting PSCs have been added to chapter 4 of the PIM.

B. Policy: N/A

II. BUSINESS REQUIREMENTS

Use"Shall" to denote a mandatory requirement

Number	Requirement	Responsibility (place an "X" in each applicable column)										
		A/B MAC	DME MAC	FI	CARRIER	DMERC	RHHI	Shared-System Maintainers				OTHER
								FISS	MCS	VMS	CWF	
5368.1	The affiliated contractors (ACs) and the Durable Medical Equipment Administrative Contractors (DME MACs) shall use the PSC support service activity codes in the Budget Performance Requirements (BPR) to report costs associated with support services provided to the PSC.		X	X	X	X	X					
5368.2	ACs, DME MACs, and A/B MACs shall follow the entire PIM for BI functions as they relate to their respective roles and areas of responsibility relating to BI and supporting the PSCs.	X	X	X	X	X	X					
5368.3	In addition to the ACs, the PSCs shall work with the MACs in all areas indicated in chapter 4 of the PIM.											PSCs
5368.4	PSC BI units shall communicate with the DME MAC, PSC, AC, and MAC medical review staff on all findings of overutilization and coordinate with the AC or MAC provider outreach and education (POE) staff to determine what, if any, education has been											PSCs

Number	Requirement	Responsibility (place an "X" in each applicable column)										
		A/B MAC	DME MAC	FI	CARRIER	DMERC	RHHI	Shared-System Maintainers				OTHER
								FISS	MCS	VMS	CWF	
	provided before any BI investigation is pursued.											
5368.5	PSC BI units shall refer any necessary provider and beneficiary outreach to the POE staff at the AC or MAC.											PSCs
5368.6	PSC BI units shall coordinate and communicate with the MR unit within your organization if a DME PSC, and coordinate and communicate with a the MR units in the AC and MACs if an A/B PSC.											PSCs
5368.7	PSC BI units shall ensure that each file contains the initial prioritization assigned and all updates.											PSCs
5368.8	Refer to section 4.2.2.6 for the revisions to PSC security.											PSCs
5368.9	PSCs shall follow the changes in chapter 4, §4.3 on MR for BI.											PSCs
5368.10	When the PSCs cannot meet the timeframes in the PIM for fulfilling OIG and DOJ law enforcement requests, the PSCs shall document all communications with the requesting offices regarding the delays.											PSCs
5368.11	If OIG and DOJ law enforcement requests require coordination with other contractors and the specified timeframes cannot be met, the PSC shall communicate with the contractors to ensure the requests are not delayed unnecessarily. The PSCs shall document these communications with other contractors.											PSCs
5368.12	PSCs shall prioritize DOJ requests into Emergency Requests, Priority I Requests, and Priority II requests as instructed in section 4.4.1H of the PIM.											PSCs
5368.13	PSC BI units should assist the AC or MAC with producing outreach items and materials for beneficiary and provider education and awareness.											PSCs
5368.14	When a Fraud Alert is officially issued, the PSC BI unit shall determine whether the scheme exists within their jurisdiction.											PSCs
5368.15	All Fraud Alerts shall be reviewed and reevaluated annually, for at least three years from the date the Fraud Alert was issued, and if											PSCs

Number	Requirement	Responsibility (place an "X" in each applicable column)										
		A/B MAC	DME MAC	FI	CARRIER	DMERC	RHHI	Shared-System Maintainers				OTHER
								FISS	MCS	VMS	CWF	
	necessary, PSC BI units shall take the appropriate actions to protect the Medicare Trust Fund.											
5368.16	All revisions to the Alert by the PSC BI unit must be done through track changes and returned to the Program Integrity Group.											PSCs
5368.17	A new requirement for data to evaluate PSC edit effectiveness via a monthly report from the AC and MAC shall be included in the JOA.	X	X	X	X	X	X					PSCs
5368.18	A new requirement for coordination on LCDs (applicable only to JOAs between DME PSCs and DME MACs) shall be included in the JOA.		X									PSCs
5368.19	A new requirement for coordination on Provider Outreach and Education shall be included in the JOA.	X	X	X	X	X	X					PSCs
5368.20	The PSCs shall accept the revised Exhibit 37 submitted by the OIG when making data requests.											PSCs

III. PROVIDER EDUCATION

Number	Requirement	Responsibility (place an "X" in each applicable column)										
		A/B MAC	DME MAC	FI	CARRIER	DMERC	RHHI	Shared-System Maintainers				OTHER
								FISS	MCS	VMS	CWF	
	None.											

IV. SUPPORTING INFORMATION

A. For any recommendations and supporting information associated with listed requirements, use the box below:
Use "Should" to denote a recommendation.

X-Ref Requirement Number	Recommendations or other supporting information:
	N/A

B. For all other recommendations and supporting information, use the space below:

V. CONTACTS

Pre-Implementation Contact(s): Kimberly Downin, Kimberly.Downin@cms.hhs.gov

Post-Implementation Contact(s): Kimberly Downin, Kimberly.Downin@cms.hhs.gov

VI. FUNDING

A. *For TITLE XVIII Contractors*, use only one of the following statements:

No additional funding will be provided by CMS; contractor activities are to be carried out within their FY 2007 operating budgets.

B. *For Medicare Administrative Contractors (MAC)*, use only one of the following statements:

The contractor is hereby advised that this constitutes technical direction as defined in your contract. We do not construe this as a change to the Statement of Work (SOW). The contractor is not obligated to incur costs in excess of the amounts specified in your contract unless and until specifically authorized by the contracting officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the contracting officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

Medicare Program Integrity Manual
Chapter 4 - Benefit Integrity

Table of Contents
(Rev. 176, 11-24-06)

4.1 - Introduction

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The Program Integrity Manual (PIM) reflects the principles, values, and priorities of the Medicare Integrity Program (MIP). The primary principle of Program Integrity (PI) is to pay claims correctly. In order to meet this goal, Program Safeguard Contractors (PSCs), Affiliated Contractors (ACs), and *Medicare Administrators Contractors (MACs)* must ensure that they pay the right amount for covered and correctly coded services rendered to eligible beneficiaries by legitimate providers. The Centers for Medicare & Medicaid Services (CMS) follows four parallel strategies in meeting this goal: 1) preventing fraud through effective enrollment and through education of providers and beneficiaries, 2) early detection through, for example, medical review and data analysis, 3) close coordination with partners, including PSCs, ACs, *MACs*, and law enforcement agencies, and 4) fair and firm enforcement policies.

Fiscal Intermediaries (FIs) and Carriers that have transitioned their Benefit Integrity (BI) work to a PSC (referred to as Affiliated Contractors or ACs) shall follow the entire PIM for BI functions as they relate to their respective roles and areas of responsibility relating to BI.

The ACs shall use the PSC support service activity codes in the Budget Performance Requirements (BPR) to report costs associated with support services provided to the PSC. *The ACs and all MACs shall follow the entire PIM for BI functions as they relate to their respective roles and areas of responsibility relating to BI and supporting the PSCs.*

The PSCs shall follow the PIM to the extent outlined in their respective task orders. The PSC shall only perform the functions outlined in the PIM as they pertain to their own operation. The PSC, in partnership with CMS, shall be proactive and innovative in finding ways to enhance the performance of PIM guidelines.

4.2 - The Medicare Fraud Program

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The primary goal of the PSC BI unit is to identify cases of suspected fraud, develop them thoroughly and in a timely manner, and take immediate action to ensure that Medicare Trust Fund monies are not inappropriately paid out and that any mistaken payments are recouped. Suspension and denial of payments and the recoupment of overpayments are an example of the actions that may be taken. All cases of potential fraud are referred to the Office of Inspector General (OIG), Office of Investigations field office (OIFO) for consideration and initiation of criminal or civil prosecution, civil monetary penalty, or administrative sanction actions. AC *and MAC* personnel conducting each segment of claims adjudication, medical review (MR), and professional relations functions shall be aware of their responsibility for identifying fraud and be familiar with internal procedures for forwarding potential fraud cases to the PSC BI unit. Any area within the AC *and MAC* (e.g., medical review, enrollment, second level screening staff) that refers potential

fraud and abuse to the PSC shall maintain a log of all these referrals. At a minimum, the log shall include the following information: provider/physician/supplier name, beneficiary name, HIC number, nature of the referral, date the referral is forwarded to the PSC BI unit, name and contact information of the individual who made the referral, and the name of the PSC to whom the referral was made.

Preventing and detecting potential fraud involves a cooperative effort among beneficiaries, PSCs, ACs, *MACs*, providers, quality improvement organizations (QIOs), state Medicaid fraud control units (MFCUs), and Federal agencies such as CMS, the Department of Health and Human Services (DHHS), OIG, the Federal Bureau of Investigation (FBI), and the Department of Justice (DOJ).

Each investigation is unique and shall be tailored to the specific circumstances. These guidelines are not to be interpreted as requiring the PSC BI units to follow a specific course of action or establishing any specific requirements on the part of the government or its agents with respect to any investigation. Similarly, these guidelines shall not be interpreted as creating any rights in favor of any person, including the subject of an investigation.

When the PSC BI unit has determined that a situation is not fraud, it shall refer these situations to the appropriate unit at the PSC, AC, or *MAC*.

4.2.1 - Examples of Medicare Fraud

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The most frequent kind of fraud arises from a false statement or misrepresentation made, or caused to be made, that is material to entitlement or payment under the Medicare program. The violator may be a provider, a beneficiary, or an employee of a provider or some other person or business entity, including a billing service or an intermediary employee.

Providers have an obligation, under law, to conform to the requirements of the Medicare program. Fraud committed against the program may be prosecuted under various provisions of the United States Code and could result in the imposition of restitution, fines, and, in some instances, imprisonment. In addition, there is also a range of administrative sanctions (such as exclusion from participation in the program) and civil monetary penalties that may be imposed when facts and circumstances warrant such action.

Fraud may take such forms as:

- Incorrect reporting of diagnoses or procedures to maximize payments.

- Billing for services not furnished and/or supplies not provided. This includes billing Medicare for appointments that the patient failed to keep.

- Billing that appears to be a deliberate application for duplicate payment for the same services or supplies, billing both Medicare and the beneficiary for the same service, or billing both Medicare and another insurer in an attempt to get paid twice.

- Altering claim forms, electronic claim records, medical documentation, etc., to obtain a higher payment amount.

- Soliciting, offering, or receiving a kickback, bribe, or rebate, e.g., paying for a referral of patients in exchange for the ordering of diagnostic tests and other services or medical equipment.

- Unbundling or "exploding" charges.

- Completing Certificates of Medical Necessity (CMNs) for patients not personally and professionally known by the provider.

- Participating in schemes that involve collusion between a provider and a beneficiary, or between a supplier and a provider, and result in higher costs or charges to the Medicare program.

- Participating in schemes that involve collusion between a provider and an AC or *MAC* employee where the claim is assigned, e.g., the provider deliberately over bills for services, and the AC or *MAC* employee then generates adjustments with little or no awareness on the part of the beneficiary.

- Billing based on "gang visits," e.g., a physician visits a nursing home and bills for 20 nursing home visits without furnishing any specific service to individual patients.

- Misrepresentations of dates and descriptions of services furnished or the identity of the beneficiary or the individual who furnished the services.

- Billing non-covered or non-chargeable services as covered items.

- Repeatedly violating the participation agreement, assignment agreement, and the limitation amount.

- Using another person's Medicare card to obtain medical care.

- Giving false information about provider ownership in a clinical laboratory.

- Using the adjustment payment process to generate fraudulent payments.

Examples of cost report fraud include:

- Incorrectly apportioning costs on cost reports.

- Including costs of non-covered services, supplies, or equipment in allowable costs.

- Arrangements by providers with employees, independent contractors, suppliers, and others that appear to be designed primarily to overcharge the program through various devices (commissions, fee splitting) to siphon off or conceal illegal profits.

- Billing Medicare for costs not incurred or which were attributable to non-program activities, other enterprises, or personal expenses.

- Repeatedly including unallowable cost items on a provider's cost report except for purposes of establishing a basis for appeal.

- Manipulation of statistics to obtain additional payment, such as increasing the square footage in the outpatient areas to maximize payment.

- Claiming bad debts without first genuinely attempting to collect payment.

- Certain hospital-based physician arrangements, and amounts also improperly paid to physicians.

- Amounts paid to owners or administrators that have been determined to be excessive in prior cost report settlements.

- Days that have been improperly reported and would result in an overpayment if not adjusted.

- Depreciation for assets that have been fully depreciated or sold.

- Depreciation methods not approved by Medicare.

- Interest expense for loans that have been repaid for an offset of interest income against the interest expense.

- Program data where provider program amounts cannot be supported.

- Improper allocation of costs to related organizations that have been determined to be improper.

- Accounting manipulations.

4.2.2 - Program Safeguard Contractor Benefit Integrity Unit

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI unit is responsible for preventing, detecting, and deterring Medicare fraud. The PSC BI unit:

- Prevents fraud by identifying program vulnerabilities.

- Proactively identifies incidents of potential fraud that exist within its service area and takes appropriate action on each case.

- Investigates (determines the factual basis of) allegations of fraud made by beneficiaries, providers, CMS, OIG, and other sources.

- Explores all available sources of fraud leads in its jurisdiction, including the MFCU and its corporate anti-fraud unit.

- Initiates appropriate administrative actions to deny or to suspend payments that should not be made to providers where there is reliable evidence of fraud.

- Refers cases to the Office of the Inspector General/Office of Investigations (OIG/OI) for consideration of civil and criminal prosecution and/or application of administrative sanctions (see PIM, chapter 4, §§4.18ff, 4.19ff, and 4.20ff).

- *Refer any necessary provider and beneficiary outreach to the POE staff at the AC or MAC.*

Initiates and maintains networking and outreach activities to ensure effective interaction and exchange of information with internal components as well as outside groups.

The PSC BI units are required to use a variety of techniques, both proactive and reactive, to address any potentially fraudulent billing practices.

Proactive (self-initiated) leads may be generated and/or identified by any internal PSC, AC, or *MAC* component, not just the PSC BI units (e.g., claims processing, data analysis, audit and reimbursement, appeals, medical review, enrollment). However, the PSC BI units shall pursue leads through data analysis (PSCs shall follow chapter 2, §2.3 for sources of data), the Internet, the Fraud Investigation Database (FID), news media, etc.

The PSC BI units shall take prompt action after scrutinizing billing practices, patterns, or trends that may indicate fraudulent billing, i.e., reviewing data for inexplicable aberrancies (other than the expected) and relating the aberrancies to specific providers, identifying “hit and run” providers, etc. PSC BI units shall meet periodically with staff from their respective internal components and PSCs shall also meet with AC *and MAC* staff to discuss any problems identified that may be a sign of potential fraud.

Fraud leads from any external source (e.g., law enforcement, CMS referrals, beneficiary complaints) are considered to be reactive and not proactive. However, taking ideas from external sources, such as non-restricted fraud alerts and using them to look for unidentified aberrancies within PSC data is proactive.

4.2.2.1 - Organizational Requirements

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Full PSCs are not required to separate their MR and BI units. However, all BI information shall be kept confidential and secure and shared with MR only on a need-to-know basis.

The PSC BI unit managers shall have sufficient authority to guide BI activities. The managers shall be able to establish, control, evaluate, and revise fraud-detection procedures to ensure their compliance with Medicare requirements.

The PSC BI unit manager shall prioritize work coming into the PSC BI unit to ensure that investigations and cases with the greatest program impact/and or urgency are given the highest priority. Allegations or cases having the greatest program impact would include cases involving:

- Patient abuse or harm.
- Multi-state fraud.
- High dollar amounts of potential overpayment.
- Likelihood for an increase in the amount of fraud or enlargement of a pattern.
- The PSCs, ACs, and *MACs* shall give high priority to fraud complaints made by Medicare supplemental insurers. If a referral by a Medigap insurer includes investigatory findings indicating fraud stemming from site reviews, beneficiary interviews and/or medical record reviews, PSC BI units shall 1) conduct an immediate data run to determine possible Medicare losses, and 2) refer the case to the OIG.
- Law enforcement requests for assistance that involve responding to court-imposed deadlines.
- Law enforcement requests for assistance in ongoing investigations that involve national interagency (DHHS -DOJ) initiatives or projects.

4.2.2.2 - Liability of Program Safeguard Contractor Benefit Integrity Unit Employees

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Under the terms of their contracts and proposed rule 42 CFR § 421.316(a), PSCs, their employees and professional consultants are protected from criminal or civil liability as a result of the activities they perform under their contracts as long as they use due care. If a PSC, or any of its employees or consultants are named as defendants in a lawsuit, CMS will determine, on a case-by-case basis, whether to request that the U.S. Attorney's office offer legal representation. If the U.S. Attorney's office does not provide legal

representation, the PSC will be reimbursed for the reasonable cost of legal expenses it incurs in connection with defense of the lawsuit as long as funds are available and the expenses are otherwise allowable under the terms of the contract.

If a PSC is served with a complaint, it shall immediately contact its chief legal counsel and GTL. The PSC shall forward the complaint to the Department of Health and Human Services Office of the regional chief counsel (CMS regional attorney) who, in turn, will notify the U.S. Attorney. The HHS office and/or the GTL will notify the PSC whether legal representation will be sought from the U.S. Attorney prior to the deadline for filing an answer to the complaint.

4.2.2.3 – Anti-Fraud Training

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

All levels of PSC employees shall know the goals and techniques of fraud detection and control in general and as they relate to their own areas of responsibility (i.e., general orientation for new employees and highly technical sessions for BI unit staff and if applicable, medical review staff). All PSC BI unit staff shall be adequately qualified for the work of detecting and investigating situations of potential fraud.

CMS National Benefit Integrity Training

Each PSC BI unit shall send the appropriate representative(s) to *CMS'* national benefit integrity training each year it is provided.

4.2.2.3.1 - Training for Law Enforcement Organizations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The FBI agents and DOJ attorneys need to understand Medicare. PSC BI units shall conduct special training programs for them upon request. PSCs should also consider inviting appropriate DOJ, OIG, and FBI personnel to existing programs intended to orient employees to PSC operations, or to get briefings on specific cases or Medicare issues.

4.2.2.4.1 - Maintain Controlled Filing System and Documentation

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall maintain files on providers who have been the subject of complaints, prepayment flagging, PSC BI unit investigations, OIG/OI and/or DOJ investigations, U.S. Attorney prosecution, and any other civil, criminal, or administrative action for violations of the Medicare or Medicaid programs. The files shall contain documented warnings and educational contacts, the results of previous investigations, and copies of complaints resulting in investigations.

The PSC BI units shall set up a system for assigning and controlling numbers at the initiation of investigations, and shall ensure that:

- All incoming correspondence or other documentation associated with an investigation contains the same file number and is placed in a folder containing the original investigation material.

- Investigation files are adequately documented to provide an accurate and complete picture of the investigative effort.

- All contacts are clearly and appropriately documented.

- *Each file contains the initial prioritization assigned and all updates.*

- Each investigation file lists the name, organization, address, and telephone numbers of all persons with whom the PSC BI unit can discuss the investigation (including those working within the PSC).

It is important to establish and maintain histories and documentation on all fraud and abuse investigations and cases. PSC BI units shall conduct periodic reviews of the kinds of fraud detected over the past several months to identify any patterns of potential fraud and abuse situations for particular providers. The PSC BI units shall ensure that all evidentiary documents are kept free of annotations, underlining, bracketing, or other emphasizing pencil, pen, or similar marks.

The PSC BI units shall establish an internal monitoring and investigation and case review system to ensure the adequacy and timeliness of fraud and abuse activities.

4.2.2.6 – Benefit Integrity Security Requirements

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

To ensure a high level of security for the PSC BI function, the PSCs shall develop, implement, operate, and maintain security policies and procedures that meet and conform to the requirements of the Business Partners Security Manual (BPSSM) and the Core Security Requirements (CSR) and its operational appendices (A, B, C, and D). The BPSSM is located at: *http://www.cms.hhs.gov/manuals/downloads/117_systems_security.pdf and the CSR is at* *http://www.cms.hhs.gov/it/security. Further, the PSCs shall adequately inform and train all PSC employees to follow PSC security policies and procedures so the information the PSC obtains is confidential.*

Please note that data PSCs collect in the administration of PSC contracts belong to CMS. Thus, PSCs collect and use individually identifiable information on behalf of the Medicare program to routinely perform the business functions necessary for administration of the Medicare program, such as, medical review and program integrity activities to prevent fraud and abuse. Consequently, any disclosure of individually identifiable information without prior consent from the individual to whom the information pertains, or without statutory or contract authority, requires CMS' prior approval.

This section discusses broad security requirements that PSCs shall follow. Most requirements listed below are in the BPSSM or CSRs and are included by reference. There are several exceptions. The first is requirement A (concerning PSC BI Unit Operations), which addresses several broad requirements; CMS has included requirement A here for emphasis and clarification. Two others are in requirement B (concerning sensitive information) and requirement G (concerning telephone security). Requirements B and G relate to security issues that are not systems related and are not in the BPSSM.

A. Program Safeguard Contractor Benefit Integrity Unit Operations

- The PSCs shall conduct their activities in areas not accessible to the general public.

- *The PSC BI unit shall completely segregate itself from all other operations. Segregation shall include floor to ceiling walls and/or other measures described in CSR 2.2.6 that prevent unauthorized persons access to or inadvertent observation of sensitive and investigative information. The only exception to this requirement is that PSCs may co-locate PSC MR and PSC BI units in the same building and same office space.* However, PS BI units shall keep all PSC BI unit information confidential and secure and shall share PSC BI unit information with PSC MR units only on need-to-know basis.

- *Other requirements regarding PSC BI unit operations shall include sections 3.1, 3.1.2, 3.10.2, 4.1.1.2, 4.2, 4.2.5, and 4.2.6 of the BPSSM.*

B. Handling and Physical Security of Sensitive *and Investigative* Material

See the BPSSM section 3.8 for definitions of sensitive and investigative material.

In addition, the PSCs shall follow the requirements provided below:

- Establish a policy that employees shall discuss specific allegations of fraud only within the context of their professional duties and only with those who have a valid need-to-know. *This may include:*

  - *Appropriate CMS personnel,*
  - Staff from the PSC, AC, or *MAC* medical review *and/or benefit integrity unit* staff,
  - PSC, AC*, or MAC audit unit staff,*
  - PSC, AC, *or MAC* data analysis staff,
  - PSC, AC*, or MAC senior management, or*
  - PSC, AC*, or MAC* corporate counsel.

- *The CSRs require that:*

  - *The following workstation security requirements are specified and implemented: (1) what workstation functions can be performed, (2) the manner in which those functions are to be performed, (3) and the physical attributes of the surrounding of a specific workstation or class of workstation that can access CMS sensitive information. CMS requires that for PSCs all the local workstations as well as the workstations used at home comply with these requirements.*
  - *If PSC employees are authorized to work at home on sensitive data, they are required to observe the same security practices that they observe at the office. These should address such items as viruses, VPNs, and protection of sensitive data as printed documents.*
  - *Users are prohibited from installing desktop modems.*
  - *The connection of portable computing or portable network devices on the CMS claims processing network is restricted to approved devices only. Removable hard drives and/or a FIPS-approved method of cryptography shall be employed to protect information residing on portable and mobile information systems.*

- *For alternate work site equipment controls, (1) only CMS Business Partner owned computers and software are used to process, access, and store sensitive information; (2) a specific room or area that has the appropriate space and facilities is used; (3) means are available to facilitate communication with their managers or other members of the Business Partner Security staff in case of security problems; (4) locking file cabinets or desk drawers; (5) "locking hardware" to secure IT equipment to larger objects such as desks or tables; and (6) smaller Business Partner-owned equipment is locked in a storage cabinet or desk when not in use. If wireless networks are used at alternate work sites, wireless base stations are placed away from outside walls to minimize transmission of data outside of the building.*

Alternate work sites are those areas where employees, subcontractors, consultants, auditors, etc. perform work associated duties. The most common alternate work site is an employee's home. However, there may be other alternate work sites such as training centers, specialized work areas, processing centers, etc.

- Ensure the mailroom, general correspondence, and telephone inquiries procedures maintain confidentiality whenever the PSC receives correspondence, telephone calls, or other communication alleging fraud. Further, all internal written operating procedures shall clearly state security procedures.

- Direct mailroom staff not to open PSC BI unit mail in the mailroom, unless the PSC has requested the mailroom do so for safety and health precautions. Alternately, if mailroom staff opens PSC BI unit mail, mailroom staff shall not read the contents.

- For mail processing sites separate from the PSC, the PSCs shall minimize the handling of PSC BI unit mail by multiple parties before delivery to the PSC BI unit.

- The PSCs shall mark mail to CO or another PSC, "personal and confidential," and address it to a specific person.

- Where more specialized instructions do not prohibit PSC BI unit employees, PSC BI employees may retain sensitive *and investigative* materials at their desks, in office work baskets, and at other points in the office during the course of the normal work day. Regardless of other requirements, the employee shall restrict access to sensitive *and investigative* materials, and PSC staff shall not leave such material unattended.

- *PSC staff shall safeguard all sensitive or investigative material when in transit.*

- The PSC BI units shall maintain a controlled filing system (see PIM, chapter 4, §4.2.2.4.1).

C. Designation of a Security Officer

The Security Officer shall take such action as is necessary to correct breaches of the security standards and to prevent recurrence of the breaches. In addition, the Security

Officer shall document the action taken and maintain that documentation for at least seven years. Actions shall include:

- *Within one hour of discovering a security incident, clearly and accurately report the incident following BPSSM requirements for reporting of security incidents. For purposes of this requirement, a security incident is the same as the definition in section 3.6, Incident Reporting and Response, of the BPSSM.*

- *Specifically, the report shall address the following where appropriate:*

    - *Types of information about beneficiaries shall at a minimum address whether the compromised information includes name, address, HICN, and date of birth.*

    - *Types of information about providers shall at a minimum address if the compromised information includes name, address, and provider ID.*

    - *Whether law enforcement is investigating any of the providers with compromised information, and*

    - *Police reports.*

- *Provide additional information that CMS requests within 72 hours of the request.*

- *If CMS requests, issue a Fraud Alert to all CMS Medicare contractors listing the HICNs and provider IDs that were compromised within 72 hours of the discovery that the data was compromised.*

- *Within 72 hours of discovery of a security incident, when feasible, review all security measures and revise them if necessary so they are adequate to protect data against physical or electronic theft.*

See section 3.1, of the BPSSM and Attachment 1 to this manual section (Letter from Director, Office of Financial Management, concerning security and confidentiality of PSC data) for additional requirements.

D. Staffing of the Program Safeguard Contractor Benefit Integrity Unit and Security Training

The PSC shall perform thorough background and character reference checks, including at a minimum credit checks, for potential employees to verify their suitability for employment with the PSC BI unit. *Specifically, background checks shall at least be at level 2 (moderate risk – people with access to sensitive data at CMS – level 5 risk). The PSC may require investigations above a level 2 if the PSC believes the higher level is required to protect sensitive information.*

At the point the PSC makes a hiring decision for a PSC BI unit position and prior to the selected person starting work, the PSC shall require the proposed candidate to fill out a conflict of interest declaration as well as a confidentiality statement.

Annually, the PSC shall require existing employees to complete a conflict of interest declaration as well as a confidentiality statement.

The PSC shall not employ temporary employees, such as those from temporary agencies, and students (non-paid or interns) in the PSC BI unit.

The PSC shall thoroughly explain to and discuss with employees special security considerations under which the PSC BI unit operates at least once a year. *Further, this training shall emphasize that in no instance shall employees disclose sensitive or investigative information even in casual conversation.*

See sections 2.0 of the BPSSM and CSRs 1.1.1-1.1.5, 1.1.7, 1.4.1, 1.6.4, 5.6.1, 5.6.3, and 6.3.4 for additional training requirements.

E. Access to Information

See section 2.3.4 of the BPSSM for requirements regarding access to PSC information.

F. Computer Security

See section 4.1.1 of the BPSSM for the computer security requirements.

G. Telephone Security

The PSC BI units shall implement phone security practices. The PSC BI units shall discuss investigations and cases only with those individuals that have a need to know the information, and shall not divulge information to individuals not personally known to the PSC BI unit involved in the investigation of the related issue.

Additionally, the PSC BI units shall only use CMS, OIG, DOJ, and FBI phone numbers that they can verify. *To assist with this requirement,* PSC management shall provide PSC BI unit staff with a list of the names and telephone numbers of the individuals of the authorized agencies that the PSC BI units deal with and shall ensure that this list is properly maintained and periodically updated.

Employees shall be polite and brief in responding to phone calls, but shall not volunteer any information or confirm or deny that an investigation is in process. *However,* PSC BI units shall not respond to questions concerning any case the OIG, FBI, or any other law enforcement agency is investigating. The PSC BI units shall refer such questions to the OIG, FBI, etc., as appropriate.

Finally, the PSC BI units shall transmit sensitive *and investigative* information via facsimile (fax) lines only after the PSC has verified that the receiving fax machine is secure. Unless the fax machine is secure, PSC BI units shall make arrangements with the addressee to have someone waiting at the receiving machine while the fax is transmitting. The PSC shall not transmit sensitive *and investigative* information via fax if the sender must delay a feature, such as entering the information into the machine's memory.

4.2.3 - Durable Medical Equipment *Medicare Administrative Contractor* Fraud Functions

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The *DME PSCs* shall process all complaints alleging DMEPOS fraud that are filed in their regions in accordance with requirements of PIM Chapter 4, §4.6ff. The BI unit manager has responsibility for all BI unit activity, including the coordination with outside organizations as specified in the PIM, chapter 4, §4.4.2.1.

A. General Requirements

Since the Medicare program has become particularly vulnerable to fraudulent activity in the DMEPOS area, each *DME* PSC shall:

- Routinely communicate with and exchange information with its *DME* PSC MR unit and ensure that referrals for prepayment MR review or other actions are made.

- Consult with the *DME PSC* medical directors workgroup in cases involving medical policy or coding issues.

- Fully utilize data available from the *MAC with the data analysis and coding function (DAC)* to identify items susceptible to fraud.

- Keep the *DAC*, *other* PSCs, *GTLs, Associate GTLs, and SMEs* informed of its ongoing activities and share information concerning aberrancies identified using data analysis, ongoing and emerging fraud schemes identified, and any other information that may be used to prevent similar activity from spreading to other jurisdictions.

4.3 – Medical Review for Benefit Integrity Purposes

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

As stated in PIM, chapter 1,sSection 1.1, the CMS' national objectives and goals as they relate to medical review are as follows: 1) Increase the effectiveness of medical review payment safeguard activities; 2) Exercise accurate and defensible decision making on medical review of claims; 3) Place emphasis on reducing the paid claims error rate by notifying the individual billing entities (i.e., providers, suppliers, or other approved clinicians) of medical review findings and making appropriate referrals to provider outreach and education (POE); and 4) Collaborate with other internal components and

external entities to ensure correct claims payment, and to address situations of potential fraud, waste, and abuse.

The statutory authority for the MR program includes sections 1812, 1816, 1832, 1833(e), 1842, 1842(a)(2)(B), 1861, 1862(a), 1862(a)(1), 1861, and 1874 of the Social Security Act (the Act). In addition, the regulatory authority for the MR program rests in 42 CFR 421.100 for intermediaries and 42 CFR 421.200 for carriers. Refer to PIM, chapter 3, for detailed information about the statutory and regulatory authorities.

The focus of MR units is to reduce the error rate through medical review and provider notification and feedback, whereas medical review for BI purposes focuses on addressing situations of potential fraud, waste and abuse.

Data analysis is an essential first step in determining whether patterns of claims submission and payment indicate potential problems. Such data analysis may include simple identification of aberrancies in billing patterns within a homogeneous group, or much more sophisticated detection of patterns within claims or groups of claims that might suggest improper billing or payment. The contractor's ability to make use of available data and apply innovative analytical methodologies is critical to the success of both MR and MR for BI purposes. See PIM, chapter 2 in its entirety for MR and BI data analysis requirements.

The PSC BI units and *DME PSC, AC, and A/B MAC* MR units shall have ongoing discussions and close working relationships regarding situations identified that may be signs of potential fraud. Intermediaries *and A/B MACs* shall also include the cost report audit unit in the ongoing discussions. *AC and A/B MAC medical review (MR) staff shall coordinate and communicate with their associated PSC BI units to ensure coordination of efforts, to prevent inappropriate duplication of review activities, and to assure contacts made by the AC or MAC are not in conflict with benefit integrity related activities.*

A. Referrals from the Medical Review Unit to the Benefit Integrity Unit

If a provider appears to have knowingly and intentionally furnished services that are not covered, or filed claims for services not furnished as billed, or made any false statement on the claim or supporting documentation to receive payment, the *DME* PSC, AC, or *MAC* MR unit personnel shall discuss this with the PSC BI unit. If the PSC BI unit agrees that there is potential fraud, the MR unit shall then make a referral to the PSC BI unit for investigation. Provider documentation that shows a pattern of repeated misconduct or conduct that is clearly abusive or potentially fraudulent despite provider education and direct contact with the provider to explain identified errors shall be referred to the PSC BI unit.

B. Referrals from the Benefit Integrity Unit to the Medical Review Unit and Other Units

The PSC BI units are also responsible for preventing and minimizing the opportunity for fraud. The PSC BI units shall identify procedures that may make Medicare vulnerable to potential fraud and take appropriate action.

The PSC BI unit may request the AC or A/B MAC to install a prepayment edit or auto-denial edit.

The PSC shall work with its own nurses to perform *MR for BI* reviews.

C. Benefit Integrity/Medical Review Determinations

When MR staff are reviewing a medical record for MR purposes, their focus is on making a coverage and/or coding determination. However, when PSC staff are performing BI-directed medical review, their focus may be different (e.g., looking for possible falsification). The PIM, chapter 3, §§ 3.4-3.4.3 outlines the procedures to be followed by both MR and MR for BI staff to make coverage and coding determinations.

1. The PSC shall maintain current references to support medical review determinations, including but not limited to:

- *Code of Federal Regulations;*
- *CMS Internet Only Manuals (IOMs);*
- *Local coverage determinations (LCDs) and/or local medical review policies (LMRPs) from the affiliated contractor (AC) or MAC;*
- *Internal review guidelines (sometimes defined as desktop procedures); and*
- *The review staff shall be familiar with the above references and able to track requirements in the internal review guidelines back to the statute or manual.*

2. The PSC shall have specific review parameters and guidelines established for the identified claims. Each claim shall be evaluated using the same review guidelines. The claim and the medical record shall be linked by identification of patient name, HIC number, diagnosis, ICN, and procedure. The PSC shall have access to provider tracking systems from medical review. The information on the tracking systems should be used for comparison to PSC findings. The PSC shall also consider that the medical review department may have established internal guidelines. (See PIM chapter 3, §3.4.4.)

3. The PSC shall evaluate if the provider specialty is reasonable for the procedure(s) being reviewed. As examples, one would not expect to see chiropractors billing for cardiac care, podiatrists for dermatological procedures, and ophthalmologists for foot care.

4. The PSC shall evaluate\determine if there is evidence in the medical record that the service submitted was actually provided and if so, if the service was medically reasonable and necessary. The PSC shall also verify diagnosis and match to age, gender, and procedure.

5. The PSC shall determine if patterns and/or trends exist in the medical record which may indicate potential fraud, waste or abuse. Examples include, but are not limited to:

- *The medical records tend to have obvious or nearly identical documentation*
- *In reviews that cover a sequence of codes (Evaluation & Management codes, therapies, radiology, etc.), there may be evidence of a trend to use the high ends codes more frequently than would be expected*
- *In a provider review, there may be a pattern of billing more hours of care than would normally be expected on a given workday*

6. The PSC shall evaluate the medical record for evidence of alterations including, but not limited to: obliterated sections, missing pages, inserted pages, white out, and excessive late entries.

7. The PSC shall document errors found and communicate these to the provider in a written format when the provider review does not find evidence of potential fraud. A referral may be made to the POE staff at the AC or MAC for additional provider education and follow-up, if appropriate.

8. The PSC shall downcode or deny, in part or in whole, depending upon the service under review when medical records do not support services billed by the provider.

9. The PSC shall thoroughly document the rationale utilized to make the medical review decision.

D. Quality Assurance

Quality assurance activities shall ensure that each element is being performed consistently and accurately throughout the PSC's MR for BI program. In addition, the PSC shall have in place procedures for continuous quality improvement. Quality Improvement builds on quality assurance in that it allows the contractor to analyze the outcomes from their program and continually improve the effectiveness of their processes.

1. The PSC shall assess the need for internal training on changes or new instructions (through minutes, agendas, sign-in sheets, etc.) and confirm with staff that they have participated in training as appropriate. The PSC staff shall have the ability to request training on specific issues.

2. The PSC shall evaluate internal mechanisms used to determine whether staff members have correctly interpreted the training (training evaluation forms, staff assessments) and demonstrated the ability to implement the instruction (internal quality assessment processes).

3. The PSC shall have an objective process to assign staff to review projects, ensuring that the correct level of expertise is available. For example, situations dealing with therapy issues may include review by an appropriate therapist or use of a therapist as a consultant to develop internal guidelines. Situations with complicated or questionable

medical issues, or where no policy exists, may require a physician consultant (medical director or outside consultant).

4. The PSC shall develop a system to address how it will monitor and maintain accuracy in decision-making (inter-reviewer reliability) as referenced in PIM, chapter 1, §1.2.3.4.

5. When the PSC evaluation results identify the need for prepayment edit placement at the AC or A/B MAC, the PSC shall have a system in place to evaluate the effectiveness of those edits on an ongoing basis as development continues.

4.4.1 - Requests for Information From Outside Organizations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Federal and state and local law enforcement agencies may seek beneficiary and provider information to further their investigations or prosecutions of individuals or businesses alleged to have committed health care fraud and other crimes for which medical records may be sought as evidence. When these agencies request that a PSC BI unit disclose beneficiary records or provider information, the responsive disclosure shall comply with applicable federal law as required by the HIPAA Business Associate provision of the PSC BI unit's contract. Federal law will dictate whether, and how much, requested information can be disclosed and disclosure will be contingent on the purpose for which it is sought, and whether information is sought about beneficiaries or providers. Certain general information, for example, which does not include specific beneficiary identifiers may be shared with a broader community (including private insurers), such as the general nature of how fraudulent practices were detected, the actions being taken, and aggregated data showing trends and/or patterns.

In deciding to share information voluntarily or in response to outside requests, the PSC BI unit shall carefully review each request to ensure that disclosure would not violate the requirements of the Privacy Act of 1974 (5 U.S.C. 552a) and/or the Privacy Rule (45 CFR, Parts 160 and 164) implemented under the HIPAA. Both the Privacy Act and the Rule seek to strike a balance that allows the flow of health information needed to provide and promote high quality health care while protecting the privacy of people who seek this care. In addition, they provide individuals with the right to know with whom their personal information has been shared and this, therefore, necessitates the tracking of any disclosures of information by the PSC BI unit. PSC BI unit questions concerning what information may be disclosed under the Privacy Act or Privacy Rule shall be directed to regional office Freedom of Information Act (FOIA)/privacy coordinator. Ultimately, the authority to release information from a Privacy Act System of Records to a third party rests with the system manager/business owner of the system of records.

The HIPAA Privacy Rule establishes national standards for the use and disclosure of individuals' health information (also called protected health information) by organizations subject to the Privacy Rule (which are called "covered entities"). As a "business associate" of CMS, PSCs are contractually required to comply with the HIPAA Privacy Rule. The Privacy Rule restricts the disclosure of any information, in any form, that can identify the recipient of medical services unless that disclosure is expressly permitted under the Privacy Rule. Two of the circumstances in which the Privacy Rule allows disclosure are for "health oversight activities" (45 CFR 164.512(d)) and "law enforcement purposes" (45 CFR 164.512 (f)), provided the disclosure meets all the relevant prerequisite procedural requirements in those subsections. Generally, protected health information may be disclosed to a health oversight agency (as defined in 45 CFR 164.501) for purposes of health oversight activities authorized by law, including administrative, civil, and criminal investigations necessary for appropriate oversight of the health care system (45 CFR 164.512(d)). The Department of Justice (DOJ), through its United States Attorneys' Offices and its headquarters-level litigating divisions, the

FBI, the Department of Health and Human Services Office of Inspector General (DHHS - OIG), and other federal, state, or local enforcement agencies, are acting in the capacity of health oversight agencies when they are investigating fraud against Medicare, Medicaid, or other health care insurers or programs.

The Rule also permits disclosures for other law enforcement purposes that are not health oversight activities but involve other specified law enforcement activities for which disclosures are permitted under HIPAA, which include a response to grand jury or administrative subpoenas and court orders, and for assistance in locating and identifying material witnesses, suspects, or fugitives. The complete list of circumstances that permit disclosures to a law enforcement agency is detailed in 45 CFR 164.512(f). Furthermore, the Rule permits covered entities, and business associates acting on their behalf, to rely on the representation of public officials seeking disclosures of protected health information for health oversight or law enforcement purposes provided that the identities of the public officials requesting the disclosure have been verified by the methods specified in the Rule (45 CFR 164.514(h)).

The Privacy Act of 1974 protects information about an individual that is collected and maintained by a federal agency in a system of records. A "record" is any item, collection, or grouping of information about an individual that is maintained by an agency. This includes, but is not limited to, information about educational background, financial transactions, medical history, criminal history, or employment history that contains a name or an identifying number, symbol, or other identifying particulars assigned to the individual. The identifying particulars can be a finger or voiceprint or a photograph. A "system of records" is any group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. For example, Medicare beneficiary data used by the PSC BI unit are maintained in a CMS "system of records" covered by the Privacy Act.

Information from some systems of records may be released only if the disclosure would be consistent with "routine uses" that CMS has issued and published. Routine uses specify who may be given the information and the basis or reason for access that must exist. Routine uses vary by the specified system of records, and a decision concerning the applicability of a routine use lies solely in the purview of the system's manager for each system of records. In instances where information is released as a routine use, the Privacy Act and Privacy Rule remain applicable. The Federal Register system of records notices maintained by CMS may be found on the Web site at http://www.cms.hhs.gov/privacyact/tblsors.asp. For example, the Department of Health and Human Services has published a routine use which permits the disclosure of personal information concerning individuals to the Department of Justice, as needed for the evaluation of potential violations of civil or criminal law and for detecting, discovering, investigating, litigating, addressing, or prosecuting a violation or potential violation of law, in health benefits programs administered by CMS. See 63, Fed. Reg. 38414, (July 16, 1998).

A. Requests from Private, Non-Law Enforcement Agencies

Generally, PSC BI units may furnish information on a scheme (e.g., where it is operating, specialties involved). Neither the name of a beneficiary or suspect can be disclosed. If it is not possible to determine whether or not information is releasable to an outside entity, PSCs shall contact their Primary Government Task Leader (GTL), Associate GTL, and SME for any further guidance.

B. Requests from Program Safeguard Contractors

The PSC BI units may furnish requested specific information on ongoing fraud investigations and on individually identifiable protected health information to any PSC, AC, or *MAC*. PSCs, ACs, and *MACs* are "business associates" of CMS under the Privacy Rule and thus are permitted to exchange information necessary to conduct health care operations. If the request concerns cases already referred to the OIG/OI, PSC BI units shall refer the requesting PSC BI unit to the OIG/OI.

C. Requests for Information from Qualified Independent Contractors

When a Qualified Independent Contractor (QIC) receives a request for reconsideration on a claim arising from a PSC review determination, it shall first coordinate with the AC *or MAC* to obtain any and all records and supporting documentation that the PSC provided to the AC *or MAC* in support of the AC's *or MAC's* first level appeals activities (redeterminations). As necessary, the QIC may also contact the PSC to discuss materials obtained from the AC *or MAC* and/or obtain additional information to support the QIC's reconsideration activities. The QIC shall send any requests to the PSC for additional information via electronic mail, facsimile, and/or telephone.

NOTE: Individually identifiable beneficiary information *shall* not be *included* in an e-mail.

These requests should be minimal. The QIC shall include in its request a name, phone number, and address to which the requested information shall be sent and/or follow-up questions shall be directed. The PSC shall document the date of the QIC's request and send/transmit the requested information within 7 calendar days of the date of the QIC's request. The date of the QIC's request is defined as the date the phone call is made (if a message is left, it is defined as the date the message was left) or the date of the e-mail request.

If a QIC identifies a situation of potential fraud and abuse, they shall immediately refer all related information to the appropriate PSC for further investigation. Refer to PIM, Exhibit 38, for QIC task orders and jurisdictions.

D. Quality Improvement Organizations and State Survey and Certification Agencies

The PSC BI units may furnish requested specific information on ongoing fraud investigations and on individually identifiable protected health information to the QIOs and State Survey and Certification Agencies. The functions QIOs perform for CMS are required by law, thus the Privacy Rule permits disclosures to them. State Survey and Certification Agencies are required by law to perform inspections, licensures, and other activities necessary for appropriate oversight of entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards, thus the Privacy Rule permits disclosures to them. If the request concerns cases already referred to the OIG/OI, PSC BI units shall refer the requestor to the OIG/OI.

E. State Attorneys General and State Agencies

The PSC BI units may furnish requested specific information on ongoing fraud investigations to state Attorneys General and to state agencies. Releases of information to these entities in connection with their responsibility to investigate, prosecute, enforce, or implement a state statute, rule or regulation may be made as a routine use under the Privacy Act of 1974, as amended; 5 USC §552a(b)(3) and 45 CFR Part 5b Appendix B (5). If individually identifiable protected health information is requested, the disclosure shall comply with the Privacy Rule. See subsection H below and PIM Exhibit 25, for guidance on how requests should be structured to comply with the Privacy Rule. PSC BI units may, at their discretion, share Exhibit 25 with the requestor as a template to assist them in preparing their request. If the request concerns cases already referred to the OIG/OI, PSC BI units shall refer the requestor to the OIG/OI.

F. Request from Medicaid Fraud Control Units

Under current Privacy Act requirements applicable to program integrity investigations, PSC BI units may respond to requests from Medicaid Fraud Control Units (MFCUs) for information on current investigations. Releases of information to MFCUs in connection with their responsibility to investigate, prosecute, enforce, or implement a state statute, rule or regulation may be made as a routine use under the Privacy Act of 1974, as amended; 5 USC §552a(b)(3) and 45 CFR Part 5b Appendix B (5). See subsection H below for further information regarding the Privacy Act requirements. If individually identifiable protected health information is requested, the disclosure shall comply with the Privacy Rule. See subsection H below and PIM Exhibit 25, for guidance on how requests should be structured to comply with the Privacy Rule. PSC BI units may, at their discretion, share Exhibit 25 with the requestor as a template to assist them in preparing their request. If the request concerns cases already referred to the OIG/OI, PSC BI units shall refer the requestor to the OIG/OI.

G. Requests from OIG/OI for Data and Other Records

The PSC BI units shall provide the OIG/OI with requested information, and shall maintain cost information related to fulfilling these requests. Such requested information may include law enforcement requests for voluntary refund data (refer to chapter 4, §4.16

for information on voluntary refunds). If major/costly systems enhancements are required to fulfill a request, the PSCs shall discuss the request with the Primary GTL, Associate GTL, and SME before fulfilling the request. These requests generally fall into one of the following categories:

Priority I – This type of request is a top priority request requiring a quick turnaround. The information is essential to the prosecution of a provider. Information or material is obtained from the PSC BI unit's files. Based on review of its available resources, the PSC BI unit shall inform the requestor what, if any, portion of the request can be provided. The PSC BI unit shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested.

The PSC BI units shall respond to such requests within 30 days *when* possible. If that timeframe cannot be met, the PSC BI unit shall notify the requesting office as soon as possible (but not later than 30 days) after receiving the request*, and the PSC shall document all communication with the requesting office regarding the delay*. PSC BI units shall include an estimate of when all requested information will be supplied. This timeframe applies to all requests with the exception of those that require Data Extract Software System (DESY) access to NCH. *If the request requires coordination with other contractors and the timeframe cannot be met, the PSC shall communicate with the contractors to ensure the request is not delayed unnecessarily. The PSC shall document these communications with other contractors.*

Priority II – This type of request is less critical than a Priority I request. Development requests may require review or interpretation of numerous records, extract of records from retired files in a warehouse or other archives, or soliciting information from other sources. Based on the review of its available resources, the PSC BI unit shall inform the requestor what, if any, portion of the request can be provided. The PSC BI unit shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested.

The PSC BI units shall respond to such requests within 45 calendar days, when possible. If that timeframe cannot be met, the PSC BI unit shall notify the requesting office within the 45-day timeframe, and include an estimate of when all requested information will be supplied. *The PSC shall document all communication with the requesting office regarding the delay. The 45-day* timeframe applies to all requests with the exception of those that require DESY access to national claims history (NCH). *If the request requires coordination with other contractors and the timeframe cannot be met, the PSC shall communicate with the contractors to ensure the request is not delayed unnecessarily. The PSC shall document these communications with other contractors.*

Disclosures of information to the OIG/OI shall comply with the Privacy Rule and Privacy Act. To comply with the Privacy Act, the OIG/OI must make all data requests using the form entitled, Office of Inspector General, Office of Investigations Data Use Agreement (see Exhibit 37). In order for CMS to track disclosures that are made to law enforcement

and health oversight agencies, PSCs and Medicare contractor BI units shall send a copy of all requests for data to the CMS Privacy Officer at the following address:

Centers for Medicare & Medicaid Services
Director of Division of Privacy Compliance Data Development
and CMS Privacy Officer
Mail Stop N2-04-27
7500 Security Boulevard
Baltimore, Maryland 21244

The information sought in the request is required to be produced to the Office of Investigations pursuant to the Inspector General Act of 1978, 5 U.S.C. App. The information is also sought by the Office of Inspector General in its capacity as a health oversight agency, and this information is necessary to further health oversight activities. Disclosure is therefore permitted under the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information, 45 CFR 164.501; 164.512(a); and 164.512(d). If the OIG provides language other than the above, the PSC shall contact the Primary GTL, Associate GTL, and SME.

H. Procedures for Sharing CMS Data With the Department of Justice

In April 1994, CMS entered into an interagency agreement with the DHHS Office of the Inspector General and the DOJ that permitted CMS contractors (PSCs) to furnish information, including data, related to the investigation of health care fraud matters directly to DOJ that previously had to be routed through OIG (see PIM Exhibit 35). This agreement was supplemented on April 11, 2003, when in order to comply with the HIPAA Privacy Rule, DOJ issued procedures, guidance, and a form letter for obtaining information (see PIM Exhibit 25). CMS and DOJ have agreed that DOJ requests for individually identifiable health information will follow the procedures that appear on the form letter (see PIM Exhibit 25). The 2003 form letter must be customized to each request. The form letter mechanism is not applicable to requests regarding Medicare Secondary Payer (MSP) information, unless the DOJ requester indicates he or she is pursuing an MSP fraud matter.

The PIM, Exhibit 25, contains the entire document issued by the DOJ on April 11, 2003. PSC BI units shall familiarize themselves with the instructions contained in this document. Data requests for individually identifiable protected health information related to the investigation of health care fraud matters will come directly from those individuals at FBI or DOJ who are involved in the work of the health care oversight agency (including, for example, from an FBI agent, AUSAs, or designee such as an analyst, auditor, investigator, or paralegal). For example, data may be sought to assess allegations of fraud; examine billing patterns; ascertain dollar losses to the Medicare program for a procedure, service, or time period; determine the nature and extent of a provider's voluntary refund(s); or conduct a random sample of claims for medical review. The law enforcement agency should begin by consulting with the appropriate Medicare contractor (usually the PSC, but possibly also the carrier, fiscal intermediary, *MAC,* or CMS) to

discuss the purpose or goal of the data request. Requests for cost report audits and/or associated documents shall be referred directly to the appropriate FI *or MAC*.

The PSC BI units shall discuss the information needed by DOJ and determine the most efficient and timely way to provide the information. When feasible, the PSC BI unit will use statistical systems to inform DOJ of the amount of dollars associated with their investigation, and the probable number of claims to expect from a claims level data run. PSC BI units shall obtain and transmit relevant statistical information to DOJ (as soon as possible but no later than five (5) working days) and advise DOJ of the anticipated volume, format, and media to be used (or alternative options, if any) for fulfilling a request for claims data.

The DOJ will confirm whether a request for claims data remains necessary based on the results of statistical analysis. If so, DOJ will discuss with CMS issues involving the infrastructure and data expertise necessary to analyze and further process the data that CMS will provide to DOJ.

If DOJ confirms that claims data are necessary, DOJ will prepare a formal request letter to the PSC BI unit with existing DOJ guidance (Exhibit 25).

The PSC BI units will provide data to DOJ, when feasible in a format to be agreed upon by the PSC BI units and DOJ. Expected time frames for fulfilling DOJ claims level data requests will depend on the respective source(s) and duration of time for which data are sought *with the exception of Emergency Requests which require coordination with Headquarters DOJ and CMS staff, these are as follows:*

Emergency Requests - Require coordination with Headquarters DOJ and CMS staff.

Priority I Requests – *This type of request is a non-emergency priority request requiring a quick turnaround. The information is essential to the prosecution of a provider. Information or material is obtained from the PSC BI unit's files. Based on review of its available resources, the PSC BI unit shall inform the requestor what, if any, portion of the request can be provided. The PSC BI unit shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested.*

The PSC BI units shall respond to such requests within 30 days when possible. If that timeframe cannot be met, the PSC BI unit shall notify the requesting office as soon as possible (but not later than 30 days) after receiving the request, and the PSC shall document all communication with the requesting office regarding the delay. PSC BI units shall include an estimate of when all requested information will be supplied. This timeframe applies to all requests with the exception of those that require Data Extract Software (DESY) access to NCH. If the request requires coordination with other contractors and the timeframe cannot be met, the PSC shall communicate with the contractors to ensure the request is not delayed unnecessarily. The PSC shall document these communications with other contractors.

Priority II Requests – *This type of request is less critical than a Priority I request. Development requests may require review or interpretation of numerous records, extract of records from retired files in a warehouse or other archives, or soliciting information from other sources. Based on the review of its available resources, the PSC BI unit shall inform the requestor what, if any, portion of the request can be provided. The PSC BI unit shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested.*

The PSC BI units shall respond to such requests within 45 calendar days, when possible. If that timeframe cannot be met, the PSC BI unit shall notify the requesting office within the 45-day timeframe, and include an estimate of when all requested information will be supplied. The PSC shall document all communication with the requesting office regarding the delay. The 45-day timeframe applies to all requests with the exception of those that require DESY access to national claims history (NCH). If the request requires coordination with other contractors and the timeframe cannot be met, the PSC shall communicate with the contractors to ensure the request is not delayed unnecessarily. The PSC shall document these communications with other contractors.

Once the format is agreed upon, the law enforcement agency will send the signed 2003 form letter, identifying the appropriate authority under which the information is being sought and specifying the details of the request to the PSC BI unit. A request for data that is submitted on the 2003 form letter is considered to be a Data Use Agreement (DUA) with CMS. In order for CMS to track disclosures that are made to law enforcement and health oversight agencies, PSC BI units shall send a copy of all requests for data to the CMS Privacy Officer at the following address:

> Centers for Medicare & Medicaid Services
> Director of Division of Privacy Compliance Data Development
> and CMS Privacy Officer
> Mail Stop N2-04-27
> 7500 Security Blvd.
> Baltimore, MD. 21244

The CMS has established a cost limit of $200,000 for any individual data request. If the estimated cost to fulfill any one request is likely to meet or exceed this figure, a CMS representative will contact the requestor to explore the feasibility of other data search and/or production options. Few, if any, individual DOJ requests will ever reach this threshold. In fact, an analysis of DOJ requests fulfilled by CMS' central office over the course of 1 year indicates that the vast majority of requests were satisfied with a minimum of expense. Nevertheless, CMS recognizes that PSC BI units may not have sufficient money in their budgets to respond to DOJ requests. In such cases, PSCs shall contact their Primary GTLs, Associate GTLs, and SMEs.

I. Law Enforcement Requests for Medical Review

The PSC BI units shall not send document request letters or go on site to providers to obtain medical records solely at the direction of law enforcement. However, if law enforcement furnishes the medical records and requests the PSC BI unit to review and interpret medical records for them, the PSC BI unit shall require law enforcement to put this request in writing. At a minimum, this request shall include the following information:

The nature of the request (e.g., what type of service is in question and what should the reviewer be looking for in the medical record)

The volume of records furnished

Due date
Format required for response

The PSC shall present the written request to the Primary GTL, Associate GTL, and SME prior to fulfilling the request. Each written request will be considered on a case-by-case basis to determine whether the *PSC has resources to fulfill the request. If so, the request may be approved*.

J. Law Enforcement Requests for PSC Audits of Medicare Provider Cost Reports Relating to Fraud

If law enforcement requests the PSC to perform an audit of a Medicare provider's cost report for fraud, the PSC shall consult with the AC *or MAC* to inquire if an audit of the cost report has already been performed. The PSC shall also consult with the Primary GTL, Associate GTL, and SME. The PSC shall provide the Primary GTL, Associate GTL, and SME with the basis for the law enforcement request and a detailed cost estimate to complete the audit. If the Primary GTL, Associate GTL, and SME approve the audit, the PSC shall perform the audit within the timeframe and cost agreed upon with law enforcement.

K. Requests from Law Enforcement for Information Crossing Several PSC Jurisdictions

If a PSC receives a request from law enforcement for information that crosses several PSC jurisdictions, the PSC shall respond back to the requestor specifying that they will be able to assist them with the request that covers their jurisdiction. However, for the information requested that is covered by another PSC jurisdiction, the PSC shall provide the requestor with the correct contact person for the inquiry, including the person's name and telephone number. Furthermore, the PSC shall inform the requestor that the Director of the Division of Benefit Integrity Management Operations at CMS CO is the contact person in case any additional assistance is needed. The PSC shall also copy their GTLs and SMEs on their response back to law enforcement for these types of cross jurisdictional requests.

L. Privacy Act Responsibilities

The 1994 Agreement and the 2003 form letter (see PIM Exhibits 35 and 25 respectively) are consistent with the Privacy Act. Therefore, requests that appear on the 2003 form letter do not violate the Privacy Act. The Privacy Act of 1974 requires federal agencies that collect information on individuals that will be retrieved by the name or another unique characteristic of the individual to maintain this information in a system of records.

The Privacy Act permits disclosure of a record, without the prior written consent of an individual, if at least one of twelve disclosure provisions apply. Two of these provisions, the "routine use" provision and/or another "law enforcement" provision, may apply to requests from DOJ and/or FBI.

Disclosure is permitted under the Privacy Act if a routine use exists in a system of records.

Both the Intermediary Medicare Claims Records, System No., 09-70-0503, and the Carrier Medicare Claims Records, System No. 09-70-0501, contain a routine use that permits disclosure to:

"The Department of Justice for investigating and prosecuting violations of the Social Security Act to which criminal penalties attach, or other criminal statutes as they pertain to Social Security Act programs, for representing the Secretary, and for investigating issues of fraud by agency officers or employees, or violation of civil rights."

The CMS Utilization Review Investigatory File, System No. 09-70-0527, contains a routine use that permits disclosure to "The Department of Justice for consideration of criminal prosecution or civil action."

The latter routine use is more limited than the former, in that it is only for "consideration of criminal or civil action." It is important to evaluate each request based on its applicability to the specifications of the routine use.

In most cases, these routine uses will permit disclosure from these systems of records; however, each request should be evaluated on an individual basis.

Disclosure from other CMS systems of records is not permitted (i.e., use of such records compatible with the purpose for which the record was collected) unless a routine use exists or one of the 11 other exceptions to the Privacy Act applies.

The law enforcement provision may apply to requests from the DOJ and/or FBI. This provision permits disclosures "to another agency or to an instrumentality of any jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record

specifying the particular portion desired and the law enforcement activity for which the record is sought."

The law enforcement provision may permit disclosure from any system of records if all of the criteria established in the provision are satisfied. Again, requests should be evaluated on an individual basis.

To be in full compliance with the Privacy Act, all requests must be in writing and must satisfy the requirements of the disclosure provision. However, subsequent requests for the same provider that are within the scope of the initial request do not have to be in writing. PSCs shall refer requests that raise Privacy Act concerns and/or issues to the Primary GTL, Associate GTL, and SME for further consideration.

M. Duplicate Requests for Information

The DOJ and the OIG will exchange information on cases they are working on to prevent duplicate investigations. If the PSC BI unit receives duplicate requests for information, the PSC BI unit shall notify the requestors. If the requestors are not willing to change their requests, the PSC BI unit shall ask the Primary GTL, Associate GTL, and SME for assistance.

N. Reporting Requirements

For each data request received from DOJ, PSC BI units shall maintain a record that includes:

The name and organization of the requestor

The date of the written request (all requests must be in writing)

The nature of the request

Any subsequent modifications to the request

Whether the Primary GTL, Associate GTL, and SME had to intervene on the outcome (request fulfilled or not fulfilled)

The cost of furnishing a response to each request

4.4.1.1 - Sharing Fraud Referrals Between the Office of the Inspector General and the Department of Justice

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall include two copies of the summary report of investigation with each fraud referral made to the OIG. As of October 18, 1999, the OI will provide one copy of the summary report of investigation along with all related information within 5

working days to the FBI Headquarters. The referral information received from the PSC BI unit includes all the information relevant to the potential fraud case. The OI will copy the PSC BI unit fraud referral to the FBI and will notify the FBI of any action they will take on the referral. The OI field offices will no longer forward health care fraud referrals directly to the local FBI field office. The OI will notify PSC BI units of its decision on the fraud referral, with specific instructions on all matters related to the referral, within 90 calendar days.

Upon receipt of fraud referrals, the OI regional field offices are required to perform one or more of the following:

- Open an investigation
- Return the matter to the PSC BI unit for further development
- Forward the referral to the local FBI office or other law enforcement agency for investigation
- Close the case with no action necessary and refer the case back to the PSC BI unit for administrative action

The PSC BI unit shall follow the instructions in PIM, Chapter 4, §4.18.1, to follow up with the OI to determine their decision after the 90-calendar-day period. The PSC BI unit is encouraged to have dialogue with law enforcement during investigations, and to discuss fraud referrals at periodic meetings. If the OI does not give the PSC BI unit a definite answer after the 90-day period, the PSC shall contact the Primary GTL, Associate GTL, and SME. The FBI will notify the PSC BI unit of their action on the PSC BI unit fraud referral within 45 calendar days from the day the FBI receives referral from the OI. However, if the PSC BI unit has not received feedback at the end of the 45-calendar-day period, the PSC BI unit may contact the applicable local FBI field office for a status. The PSC BI unit shall not contact the FBI Headquarters for a status of the fraud referral. In the case of multiple providers or servicing PSC BI units, the FBI will notify the PSC BI unit that initiated the referral as to the decision.

4.4.2.1 - Program Safeguard Contractor Coordination With Other Program Safeguard Contractors

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall coordinate with other PSC BI units within their service area. This includes sharing local coverage determinations (LCDs), and collaborating on abusive billing situations that may be occurring in multi-state PSCs. Coordination is also necessary because certain findings of fraud involving a provider could have a direct effect on payments made by ACs or *MACs*. PSCs use the appropriate staff member(s) to share information with *PSCs* not in contiguous states.

4.4.2.1 - Program Safeguard Contractor Coordination With Other Entities

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall establish and should maintain formal and informal communication with state survey agencies, OIG, DOJ, General Accounting Office (GAO), Medicaid, other Medicare contractors, other PSCs, and other organizations as applicable to determine information that is available and that should be exchanged to enhance PI activities.

If a PSC BI unit identifies a potential quality problem with a provider or practitioner in its area, it shall refer such cases to the appropriate entity, be it the QIO, state medical board, state licensing agency, etc. Any provider-specific information shall be handled as confidential information.

4.4.3 - Beneficiary, Provider, Outreach Activities

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units should *assist the AC or MAC with* produc*ing* a wide variety of outreach items and materials for beneficiary and provider education and awareness. These items should include: brochures, flyers, stuffers, pens, pencils, newspaper advertisements, public service announcements, pamphlets, and videos, to list a few.

4.5 - The ARGUS System

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

ARGUS is a user-friendly personal computer software package developed by the OIG both to access provider claims data and to limit the need for the OIG to submit multiple requests to carriers *or MACs* for claims data. ARGUS is a useful tool for reviewing relationships of data that carriers *or MACs* have available. The billing practices of physicians, for example, can be compared to that of their peers as a means of detecting aberrant behavior.

The OIG and other authorized federal law enforcement agencies request claims data as they have in the past, but do not specify how the data is to be sorted. They specify the providers and the dates of service. ARGUS, which is written in DBASE, utilizes line item claims data provided by Medicare carriers *or MACs* in a simple ASCII format and separates the incoming data into database fields.

An investigative file in ARGUS is a database file consisting of individual line items of service taken from health insurance claims forms. Each line item consists of 29 fields and 160 bytes of information. Line items from a single provider or from multiple providers involved in a specific investigation may be combined into one ARGUS file.

The PSCs are not required to have ARGUS, but they may obtain it if they wish.

When PSC BI units receive a request for data utilizing ARGUS, they complete the data elements contained in PIM Exhibit 34 (ARGUS Field Descriptions and Codes), in the order shown, and consistent with the following data conventions:

- All character fields are left-justified
- Leading zeros and blanks are omitted
- All numeric fields are right-justified
- Money fields are shown as $$$cc (no decimal point)
- All dates are shown as YYMMDD

Data are to be furnished in the above format on 3½-inch, high-density floppy disks or a compact disk. If the data does not fit on the 3½-inch disk without data compression, carriers compress the data using the PKZIP compression utility. Data will be transmitted to OIG in a format consistent with CMS's security requirements.

4.6.2 - Complaint Screening

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

This section delineates the responsibility for the BCC, PSCs, ACs, and MACs with regard to screening complaints alleging fraud and abuse. This supersedes any language within the Joint Operating Agreements (JOAs).

A. Beneficiary Contact Center, Affiliated Contractor and Medicare Administrative Contractor Responsibilities

The BCC, AC, and MAC shall be responsible for screening all complaints of potential fraud and abuse. This screening shall occur in the two phases described below.

Initial Screening – Beneficiary Contact Center

The CSRs at the BCC shall try to resolve as many inquiries as possible in the Initial Screening with data available in their desktop system. The following are some scenarios that a CSR may receive and resolve in the initial phone call rather than refer to second-level screening (this is not an all-inclusive list):

Lab Tests – CSRs shall ask the caller if they recognize the referring physician. If they do, remind the caller that the referring physician may have ordered some lab work for them. The beneficiary usually does not have contact with the lab because specimens are sent to the lab by the referring physician office. (Tip: ask if they remember the doctor withdrawing blood or obtaining a tissue sample on their last visit.)

Anesthesia Services - CSRs shall check the beneficiary claims history for existing surgery or assistant surgeon services on the same date. If a surgery charge is on file, explain to the caller that anesthesia service is part of the surgery rendered on that day.

Injections - CSRs shall check the beneficiary claim history for the injectable (name of medication) and the administration. Most of the time, administration is not payable (bundled service) (Part B only). There are very few exceptions to pay for the administration.

Services for Spouse - If the beneficiary states that services were rendered to his/her spouse and the Health Insurance Claim Numbers (HICNs) are the same, with a different suffix, the CSR shall initiate the adjustment and the overpayment process.

Billing Errors - If the beneficiary states that he/she already contacted his/her provider and the provider admitted there was a billing error, and the check is still outstanding, the CSR shall follow the normal procedures for resolving this type of billing error.

Services Performed on a Different Date - The beneficiary states that service was rendered, but on a different date. This is not a fraud issue. An adjustment to the claim may be required to record the proper date on the beneficiary's file.

Incident to Services - Services may be performed by a nurse in a doctor's office as "incident to." These services are usually billed under the physician's provider identification number (PIN) (e.g., blood pressure check, injections). These services may be billed under the minimal Evaluation and Management codes.

Billing Address vs. Practice Location Address - The CSR shall check the practice location address, which is where services were rendered. Many times the Medicare Summary Notice will show the billing address and this causes the beneficiary to think it is fraud.

X-rays with Modifier 26 - The CSRs shall ask the caller if he/she recognizes the referring physician. If so, the CSR shall explain to the caller that whenever modifier 26 is used, the patient has no contact with the doctor. The CSR shall further explain that the provider billing with modifier 26 is the one interpreting the test for the referring physician.

The CSRs shall use proper probing questions and shall utilize claim history files to determine if the case needs to be referred for second-level screening.

Any provider inquiries regarding potential fraud and abuse shall be forwarded immediately to the second-level screening staff at the AC or MAC for handling.

Any immediate advisements (e.g., inquiries or allegations by beneficiaries or providers concerning kickbacks, bribes, a crime by a Federal employee, indications of contractor employee fraud (e.g., altering claims data or manipulating it to create preferential treatment to certain providers; improper preferential treatment in collection of overpayments; embezzlement)) shall be forwarded immediately to the second-level screening staff at the AC or MAC for handling.

Second-Level Screening – AC or MAC

When the complaint/inquiry cannot be resolved by the CSR at the BCC, the issue shall be referred for more detailed screening, resolution, or referral, as appropriate, to the AC or MAC. The second-level screening staff at the AC or MAC shall only screen potential fraud and abuse complaints with a paid amount of $100 or greater (include the deductible as payment) or 3 or more beneficiary complaints (regardless of dollar amount) on the same provider. Each complaint shall be tracked and retained for 1 year. If the beneficiary inquires about the complaint, advise the beneficiary that the complaint will be tracked and if additional complaints are received a more in-depth review will be opened. The second-level screening staff at the AC and MAC shall maintain a log of all potential fraud and abuse inquiries received from the initial screening staff. At a minimum, the log shall include the following information:

Beneficiary name

Provider name

Beneficiary HIC#

Nature of the Inquiry

Date received from the initial screening staff

Date referral is sent to the PSC

Destination of the referral (i.e., name of PSC)

Documentation that an inquiry received from the initial screening staff was not forwarded to the PSC BI Unit and an explanation why (e.g., inquiry was misrouted or inquiry was a billing error that should not have been referred to the second-level screening staff).

Date inquiry is closed

The AC or MAC staff shall call the beneficiary or the provider, check claims history, and check provider correspondence files for educational/warning letters or contact reports that relate to similar complaints, to help determine whether or not there is a pattern of potential fraud and abuse. The AC or MAC shall request and review certain documents, as appropriate, from the provider, such as itemized billing statements and other pertinent information. If the AC or MAC is unable to make a determination on the nature of the complaint (e.g., fraud and abuse, billing errors) based on the aforementioned contacts and documents, the AC or MAC shall order medical records and limit the number of medical records ordered to only those required to make a determination. If the medical records are not received within 45 business days, the claim(s) shall be denied (if fraud is suspected when medical records are not received, these situations shall be referred to the PSC BI unit. The second-level screening staff shall only perform a billing and document review on medical records to verify and validate that services were rendered. If fraud and abuse are suspected after performing the billing and document review, the medical record shall be forwarded to the PSC BI unit for clinician review. If the AC or MAC staff determines that the complaint is not a fraud and/or abuse issue, and if the staff discovers that the complaint has other issues (e.g., medical review, enrollment, claims processing), it shall be referred to the appropriate department. If the AC or MAC second-level screening staff determines that the complaint is a potential fraud and abuse situation, the second-level screening staff shall forward it to the PSC BI unit for further development within 45 business days of the date of receipt from the initial screening staff, or within 30 business days of receiving medical records and/or other documentation, whichever is later. The AC or MAC shall refer immediate advisements received by beneficiaries or providers and potential fraud or abuse complaints received by current or former provider employees immediately to the PSC BI unit for further development.

The AC or MAC shall be responsible for screening all Harkin Grantees or Senior Medicare Patrol complaints for fraud. If after conducting second level screening, the AC or MAC staff determines that the complaint is a potential fraud and abuse situation, the

complaint shall be sent to the PSC BI unit within 45 business days of the date of receipt from the initial screening staff, or within 30 business days of receiving medical records and/or other documentation, whichever is later. The complainant shall be clearly identified to the PSC BI unit as a Harkin Grantees or Senior Medicare Patrol complaint. The AC or MAC shall be responsible for entering all initial referrals identified in the second-level screening area and any updates received from the PSC BI unit into the Harkin Grantees Tracking System (HGTS).

The AC or MAC shall be responsible for downloading and screening complaints from the OIG Hotline Database, and for updating the database with the status of all complaints. If the AC or MAC determines that the complaint is a potential fraud and abuse situation, the second-level screening staff shall forward it to the PSC BI unit for further development within 45 business days of receipt, or within 30 business days of receiving medical records and/or other documentation, whichever is later, just like all other complaints. The PSC BI unit shall be responsible for updating the valid cases that have been referred. PSCs shall control all OIG Hotline referrals by the OIG Hotline number (the "H" or "L" number) as well as by any numbers used in the tracking system. PSCs shall refer to this number in all correspondence to the RO.

Complaints shall be forwarded to the PSC BI unit for further investigation under the following circumstances (this is not intended to be an all inclusive list):

Claims forms may have been altered or upcoded to obtain a higher reimbursement amount.

It appears that the provider may have attempted to obtain duplicate reimbursement (e.g., billing both Medicare and the beneficiary for the same service or billing both Medicare and another insurer in an attempt to be paid twice). This does not include routine assignment violations. An example for referral might be that a provider has submitted a claim to Medicare, and then in 2 days resubmits the same claim in an attempt to bypass the duplicate edits and gain double payment. If the provider does this repeatedly and the AC or MAC determines this is a pattern, then it shall be referred.

Potential misrepresentation with respect to the nature of the services rendered, charges for the services rendered, identity of the person receiving the services, identity of persons or doctor providing the services, dates of the services, etc.

Alleged submission of claims for non-covered services are misrepresented as covered services, excluding demand bills and those with Advanced Beneficiary Notices (ABNs).

Claims involving potential collusion between a provider and a beneficiary resulting in higher costs or charges to the Medicare program.

Alleged use of another person's Medicare number to obtain medical care.

Alleged alteration of claim history records to generate inappropriate payments.

Alleged use of the adjustment payment process to generate inappropriate payments.

Any other instance that is likely to indicate a potential fraud and abuse situation.

When the above situations occur, and it is determined that the complaint needs to be referred to the PSC BI unit for further development, the AC or MAC shall prepare a referral package that includes, at a minimum, the following:

Provider name, provider number, and address.

Type of provider involved in the allegation and the perpetrator, if an employee of the provider.

Type of service involved in the allegation.

Place of service.

Nature of the allegation(s).

Timeframe of the allegation(s).

Narration of the steps taken and results found during the AC's or MAC's screening process (discussion of beneficiary contact, if applicable, information determined from reviewing internal data, etc.).

Date of service, procedure code(s).

Beneficiary name, beneficiary HICN, telephone number.

Name and telephone number of the AC or MAC employee who received the complaint.

NOTE: Since this is not an all-inclusive list, the PSC BI unit has the right to request additional information in the resolution of the complaint referral or the subsequent development of a related case (e.g., provider enrollment information).

When a provider inquiry or complaint of potential fraud and abuse or immediate advisement is received, the second-level screening staff will not perform any screening, but will prepare a referral package and send it immediately to the PSC BI unit. The referral package shall consist of the following information:

Provider name and address.

Type of provider involved in the allegation and the perpetrator, if an employee of a provider.

Type of service involved in the allegation.

Relationship to the provider (e.g., employee or another provider).

Place of service.

Nature of the allegation(s).

Timeframe of the allegation(s).

Date of service, procedure code(s).

Name and telephone number of the AC or MAC employee who received the complaint.

The AC and MAC shall maintain a copy of all referral packages.

The AC shall report all costs associated with second-level screening of inquiries for both beneficiaries and providers in Activity Code 13201. Report the total number of second-level screening of beneficiary inquiries that were closed in workload column 1; report the total number of medical records ordered for beneficiary inquiries that were closed in workload column 2; and report the total number of potential fraud and abuse beneficiary complaints identified and referred to the PSC BI unit in workload column 3. The AC shall keep a record of the cost and workload for all provider inquiries of potential fraud and abuse that are referred to the PSC BI unit in Activity Code 13201/01.

B. Program Safeguard Contractor Benefit Integrity Unit Responsibilities

At the point the complaint is received from the AC or MAC screening staff, the PSC BI unit shall further investigate the complaint, resolve the complaint investigation, or make referrals as needed to appropriate law enforcement entities or other outside entities.

The PSC BI unit shall send acknowledgement letters for complaints received from the AC or MAC to the complainant. The AC or MAC shall screen and forward the complaints within 45 business days from the date of receipt by the second level screening staff, or within 30 business days of receiving medical records and/or other documentation, whichever is later, to the PSC BI unit. The PSC BI unit shall send the acknowledgement letter within 15 calendar days of receipt of the complaint referral from the AC or MAC second-level screening staff, unless it can be resolved sooner. The letter shall be sent on PSC letterhead and shall contain the telephone number of the PSC BI unit analyst handling the case.

If the PSC BI unit staff determines, after investigation of the complaint, that it is not a fraud and/or abuse issue, but has other issues (e.g., medical review, enrollment, claims processing), it shall be referred to the AC or MAC area responsible for second-level screening, or if applicable, the appropriate PSC unit for further action. This shall allow the AC or MAC screening area to track the complaints returned by the PSC BI unit. However, the PSC BI unit shall send an acknowledgement to the complainant, indicating that a referral is being made, if applicable, to the appropriate PSC, or to the appropriate AC or MAC unit for further action.

The PSC BI unit shall communicate any updates as a result of their investigation on Harkin Grantees or Senior Medicare Patrol complaints to the AC or MAC second-level screening staff, who shall update the database accordingly.

The PSC BI unit shall update valid cases that have been referred from the OIG Hotline Database by the AC or MAC second-level screening area.

The PSC BI unit shall send the complainant a resolution letter within 7 calendar days of the resolution on the complaint investigation and/or case in accordance with PIM, chapter 4, §4.8.

4.6.3 -Filing Complaints

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall file complaints in the investigation file (refer to the sections below on investigations) that originated from the complaint, and check each against PSC BI unit files for other complaints involving the same provider.

PSC BI units shall resolve any potential fraud or abuse situations without referral to OIG/OI, if possible, and maintain all documentation on these complaint investigations for subsequent review by CMS personnel or OIG/OI.

A. Source of Complaint

Record the name and telephone number of the individual (or organization) that provided the information concerning the alleged fraud or abuse. Also list the provider's name, address, and ID number.

B. Nature of Complaint

Briefly describe the nature of the alleged fraud or abuse (e.g., “Provider billed for services not furnished,” or “Beneficiary alleged provider billed for more than deductible and coinsurance”).

Also include the following information:

- The date the complaint was received.

- A brief description of the action taken to close out the complaint. For example, "Reviewed records and substantiated amounts billed beneficiary." Insure that sufficient information is provided to enable the OIFO or the RO to understand the reason for the closeout.

- The date the complaint was closed.

- The number of complaints received to date concerning this provider, including the present complaint. This information is useful in identifying providers that are involved in an undue number of complaints.

4.7 - Investigations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

An investigation is the analysis performed on both proactive and reactive leads (e.g., complaints, data analysis, newspaper articles) in an effort to substantiate the lead or allegation as a case. However, not all investigations will result in cases.

When PSC BI units receive an allegation of fraud, or identify a potentially fraudulent situation, they shall investigate to determine the facts and the magnitude of the alleged fraud. They shall also conduct a variety of reviews to determine the appropriateness of payments, even when there is no evidence of fraud. Prioritization of the investigation workload is critical to ensure that the resources available are devoted primarily to high-priority investigations. (Complaints by current or former employees require immediate advisement to the OIG/OI. OIG/OI may request that PSC BI units perform only limited internal investigation and then immediately refer the case to them.)

The PSC BI units shall maintain files on all investigations. The files shall be organized by provider or supplier and shall contain all pertinent documents, e.g., original referral or complaint, investigative findings, reports of telephone contacts, warning letters, documented discussions, any data analysis or analytical work involving the potential subject or target of the investigation, and decision memoranda regarding final disposition of the investigation (refer to §4.2.2.4.2, for retention of these documents).

Under the terms of their contract, PSCs shall investigate potential fraud on the part of providers, suppliers, and other entities who receive reimbursement under the Medicare program for services rendered to beneficiaries. PSCs shall refer potential fraud cases to law enforcement and provide support for these cases. In addition, PSCs may provide data and other information related to potential fraud cases initiated by law enforcement when the cases involve entities or individuals who receive reimbursement under the Medicare program for services rendered to beneficiaries.

The work a PSC performs under its contract does not extend to investigations of ACs or MACs. PSCs are not authorized to assist a law enforcement agency that may be investigating allegations of fraud or other misconduct against an AC or MAC. Requests

for assistance of this nature shall be directed to the CMS CO Contractor Compliance Officer, Office of Acquisition and Grants Management.

4.7.1 – Conducting Investigations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

When the complaint cannot be dismissed by the AC or *MAC* second-level screening staff as an error or a misunderstanding, unless otherwise advised by law enforcement, PSC BI units shall use one or more of the following investigative methods to determine whether or not there is a pattern of submitting false claims. (The list is not intended to be all-inclusive.)

- Review a small sample of claims submitted within recent months. Depending on the nature of the problem, the PSC BI unit may need to request medical documentation or other evidence that would validate or cast doubt on the validity of the claims.

- Interview by telephone a small number of beneficiaries. Do not alarm the beneficiaries or imply that the provider did anything wrong. The purpose is to determine whether there appear to be other false claims or if this was a one-time occurrence.

- Look for past contacts by the PSC BI unit, or the MR unit concerning comparable violations. Also, check provider correspondence files for educational/warning letters or for contact reports that relate to similar complaints. Review the complaint file. Discuss suspicions with MR and audit staff, as appropriate.

- Perform data analysis (PSCs shall follow Chapter 2, §2.3 for sources of data).

- Review telephone calls or written questionnaires to physicians, confirming the need for home health services or DME.

- Perform random validation checks of physician licensure.

- Review original CMNs.

- Perform an analysis of high frequency/high cost, high frequency/low cost, low frequency/low cost, and low frequency/high cost procedures and items.

- Perform an analysis of local patterns/trends of practice/billing against national and regional trends, beginning with the top 30 national procedures for focused medical review and other kinds of analysis that help to identify cases of fraudulent billings.

- Initiate other analysis enhancements to authenticate proper payments.

- Perform a compilation of documentation, e.g., medical records or cost reports.

Using internal data, PSC BI units may determine the following:

- Type of provider involved in the allegation and the perpetrator, if an employee of the provider.

- Type of services involved in the allegation.

- Places of service.

- Claims activity (including assigned and non-assigned payment data in the area of the fraud complaint).

- The existence of statistical reports generated for the Provider Audit List (PAL) or other MR reports, to establish if this provider's practice is exceeding the norms established by their peer group (review the provider practice profile).

- Whether there is any documentation available on prior complaints. Obtain the appropriate Form CMS-1490s and/or 1500s, UB-92s, electronic claims and/or attachments. Review all material available.

NOTE: Due to evidentiary requirements, do not write on these forms/documents in any manner.

After reviewing the provider's background, specialty and profile, PSC BI units decide whether the situation, is potential fraud or may be more accurately categorized as a billing error. For example, records indicate that a physician has billed, in some instances, both Medicare and the beneficiary for the same service. Upon review, a BI unit determines that, rather than attempting to be paid twice for the same service, the physician made an error in his/her billing methodology. Therefore, this would be considered a determination of improper billing, rather than fraud involving intentional duplicate billing.

The purpose of these activities is to decide whether it is reasonable to spend additional investigative resources. If there appears to be a pattern, the PSC BI unit shall discuss it with OIG/OI at the onset of the investigation. The PSC BI unit shall discuss with OIG/OI the facts of the investigation and obtain OIG’s recommendation on whether or not the investigation should be further developed for possible case referral to OIG/OI.

Once a case has been referred to law enforcement, the PSC BI unit shall not contact the provider or their office personnel. If there is belief that provider contact is necessary, the PSC BI unit shall consult with OIG/OI. OIG/OI will consider the situation and, if warranted, concur with such contact.

Additionally, if the suspect provider hears that its billings are being reviewed or learns of the complaint and contacts the PSC BI unit, they shall report such contact immediately to OIG/OI.

NOTE: If investigations do not result in a case, the PSC BI unit shall take all appropriate action in order to prevent any further payment of inappropriate claims and to recover any overpayments that may have been made (the PSC BI unit shall refer to chapter 3, §3.8ff for overpayments).

4.7.2 – Closing Investigations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

An investigation shall be closed if it becomes a case (i.e., it is referred to OIG, DOJ, FBI, or AUSA), if it is referred back to the AC, *MAC,* or to another PSC due to an incorrect referral or misrouting, or if it is closed with administrative action (refer to §4.11.2.8 for FID instructions on closing investigations).

4.8 - Disposition of Cases

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

A case exists when the PSC BI unit has referred a fraud allegation to law enforcement, including but not limited to documented allegations that: a provider, beneficiary, supplier, or other subject a) engaged in a pattern of improper billing, b) submitted improper claims with suspected knowledge of their falsity, or c) submitted improper claims with reckless disregard or deliberate ignorance of their truth or falsity. This definition of a case includes any and all allegations (regardless of dollar threshold or subject matter) where PSC BI unit staff verify to their own satisfaction that there is potential Medicare fraud (the allegation is likely to be true) and a referral to law enforcement has been performed. PSC BI units do not prove fraud; such action is within the purview of the Department of Justice.

Immediate advisements shall not be considered cases (see PIM Chapter 4, §4.18.1.2).

The PSC BI units shall summarize the case and shall send two copies of the summary report of investigation, with the case file, to OIG/OI. PSC BI units shall ensure that case material is filed in an organized manner (e.g., chronological order, all pages attached with prongs or other binding material, and in the same order as summarized). When necessary, include copies of the claims (with attachments) at issue as well as copies of documentation of all educational/warning contacts with the provider that relate to this issue. See PIM Chapter 4, §4.18.1ff (Referral of Cases to Office of Inspector General/Office of Investigations) for further instruction on referrals to OIG/OI.

There may be instances when law enforcement requests that an investigation be referred before completion of the PSC BI unit investigation and case referral package. When this occurs, the PSC BI unit shall request law enforcement to send a letter or e-mail requesting immediate referral and acknowledging that the PSC BI unit did not complete their investigation and referral package. However, the PSC BI unit shall continue their investigation even though an expedited referral has been made to law enforcement in order to determine the appropriate administrative actions.

Once the case has been referred to OIG/OI, inform the complainant within 7 calendar days that the case has been referred to OIG/OI, and that further requests concerning the matter should be referred to OIG/OI. However, some cases may be sensitive and the complainant is not to be informed of the referral to OIG/OI. The PSC BI unit shall contact OIG/OI before responding to the complainant if the case is a sensitive one. Otherwise, provide the complainant with the address of OIG/OI and the name of a contact person.

Also, PSC BI units should notify the complainant within 7 calendar days of OIG/OI completing the case. OIG/OI will make a determination as to whether or not the case is to be referred to the FBI or other law enforcement agency for disposition. If adverse action is subsequently taken against the provider, explain to the complainant the action taken. Thank the complainant for his/her interest and diligence.

4.8.1 – Reversed Denials by Administrative Law Judges on Open Cases

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

If a case is still pending at the OIG, FBI, or AUSA, and denials are reversed by an Administrative Law Judge (ALJ), PSC BI units should recommend to CMS that it consider protesting the ALJ's decision to pay to the DHHS Appeals Council, which has the authority to remand or reverse the ALJ's decision. PSC BI units should be aware, however, that ALJs are bound only by statutory and administrative law (federal regulations), CMS rulings, and National Coverage Determinations.

The New York and Dallas ROs coordinate these protests. PSCs shall consult with their Primary GTL, Associate GTL, and SME before initiating a protest of an ALJ's decision. They should be aware that the Appeals Council has only 60 days in which to decide whether to review an ALJ's decisions. Thus, CMS needs to protest the ALJ decision within 30 days of the decision, to allow the Appeals Council to review within the 60-day limit. PSC BI units shall notify all involved parties immediately if they learn that claims/claim denials have been reversed by an ALJ in a case pending prosecution.

4.9.1 - Incentive Reward Program General Information

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The Medicare program will make a monetary reward only for information that leads to a minimum recovery of $100 of Medicare funds from individuals and entities determined by the CMS to have committed sanctionable offenses. Referrals from PSC BI units to the OIG made pursuant to the criteria set forth in PIM, chapter 4, §4.19ff are considered sanctionable for the purpose of the IRP.

4.9.2 - Information Eligible for Reward

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The information must relate to a specific situation, individual, or entity, and must specify the time period of the alleged activities. It must be relevant material information that directly leads to the imposition of a sanction, and non-frivolous. CMS does not give a reward for information relating to an individual or entity that, at the time the information is provided, is already the subject of a review or investigation by CMS, its PSC BI units, the OIG, the DOJ, the FBI, or any other federal, state or local law enforcement agency.

4.9.3 - Persons Eligible to Receive a Reward

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The complainant shall be determined to be eligible for a reward only if the initial complaint was received on or after July 8, 1998 and provides information that leads to a sanctionable offense as described in PIM Chapter 4, §4.19ff and Chapter 4, §4.6ff. In general, a reward is payable to all eligible individuals whose complaints were integral to the opening of a BI case. Where multiple complaints have been received, the following guidelines shall be used:

- Only complaints directly relevant to the issue/allegation investigated are eligible.
- In situations where two or more complaints of the same nature concerning the same provider/entity are received, all complaints may be eligible to share an equal portion of the reward not to exceed the maximum amount of the reward.
- The reward shall be paid to the complainant(s) who provided sufficient, specific information to open the case as discussed above.

The PSC BI unit shall make a determination of eligibility for a reward as appropriate.

4.9.4 - Excluded Individuals

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The following individuals are not eligible to receive a reward under the IRP:

- An individual who was, or is, an immediate family member of an officer or employee of the Department of Health and Human Services, its PSCs, ACs, *MACs*, or subcontractors, the Social Security Administration (SSA), the OIG, a state Medicaid agency, the DOJ, the FBI, or any other federal, state, or local law enforcement agency at the time he or she came into possession, or divulged information leading to a recovery of Medicare funds. Immediate family is as defined in 42 CFR 411.12(b), which includes any of the following:

    - Husband or wife

    - Natural or adoptive parent, child, or sibling

    - Stepparent, stepchild, stepbrother, or stepsister

    - Father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, or sister-in-law

    - Grandparent or grandchild.

- Any other federal or state employee, PSC, AC, *MAC*, or subcontractor, or DHHS grantee, if the information submitted came to his/her knowledge during the course of his/her official duties.

- An individual who received a reward under another government program for the same information furnished.

- An individual who illegally obtained the information he/she submitted.

- An individual who participated in the sanctionable offense with respect to which payment would be made.

4.9.6 - Program Safeguard Contractor Responsibilities

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

For PSCs and ACs *or PSCs and MACs*, the IRP responsibilities explained below shall be worked out in the Joint Operating Agreement.

4.9.6.1 - Guidelines for Processing Incoming Complaints

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

On or after **July 8, 1998**, any complaints received that pertain to a potentially sanctionable offense as defined by §§1128, 1128A, or 1128B of the Act, or that pertain to those who have otherwise engaged in sanctionable fraud and abuse against the Medicare program under title XVIII of the Act, are eligible for consideration for reward under the IRP. While the complainant may not specifically request to be included in the IRP, the PSC BI unit should consider the complainant for the reward program. Complaints may originate from a variety of sources such as the OIG Hotline, the PSC BI unit, customer service representatives, etc. PSCs, ACs, and *MACs* shall inform their staff of this program so they will respond to or refer questions correctly. PIM Exhibit 5 provides IRP background information to assist staff who handle inquiries. PSCs, ACs, and *MACs*, shall treat all complaints as legitimate until proven otherwise. They shall refer incoming complaints to the PSC BI unit for investigation. Complaints shall either be resolved by the PSC BI unit or, if determined to be a sanctionable offense, referred to the OIG for investigation. Complaints that belong in another PSC's jurisdiction shall be recorded and forwarded to the appropriate PSC. All information shall be forwarded to them according to existing procedures.

If an individual registers a complaint about a Medicare Managed Care provider, PSCs, ACs, and *MACs* shall record and forward all information to:

> Centers for Medicare & Medicaid Services
> Centers for Medicare Management
> Performance Review Division
> Mail Stop C4-23-07
> 7500 Security Blvd.
> Baltimore, MD 21244

4.9.6.2 - Guidelines for Incentive Reward Program Complaint Tracking

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSCs shall continue to track all incoming complaints potentially eligible for reward in their existing internal tracking system. The following complainant information shall be included:

- Name;

- Health insurance claim number or Social Security number (for non-beneficiary complaints);

- Address;

- Telephone number; or

Any other requested identifying information needed to contact the individual.

The PSC BI units shall refer cases to the OIG for investigation if referral criteria are met according to PIM Chapter 4, §4.18.1 - Referral of Cases to the Office of the Inspector General (OIG). The case report shall also be forwarded to the OIG.

The PSC BI unit shall enter all available information into the IRP tracking database. Information that shall be maintained on the IRP tracking database includes:

- Date the case is referred to the OIG.

- OIG determination of acceptance.

- If accepted by OIG, the date and final disposition of the case by the OIG (e.g., civil monetary penalty (CMP), exclusion, referral to DOJ).

- Any provider identifying information required in the FID, e.g., the Unique Physician Identification Number (UPIN).

The OIG has 90 calendar days from the referral date to make a determination for disposition of the case. If no action is taken by the OIG within the 90 calendar days, the PSC BI unit should begin the process for recovering the overpayment and issuance of the reward, if appropriate.

4.9.6.3 - Overpayment Recovery

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall initiate overpayment recovery actions according to PIM Chapter 3, §3.8ff, if it is determined an overpayment exist. Only ACs or *MACs* shall issue demand letters and recoup the overpayment.

4.9.6.4 - Eligibility Notification

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

After all fraudulently obtained Medicare funds have been recovered and all fines and penalties collected, if appropriate, the PSC BI unit will send a reward eligibility notification letter and a reward claim form to the complainant by mail at the most recent address supplied by the individual. PIM Exhibit 5.1 provides a sample eligibility

notification letter and Exhibit 5.2 provides a sample reward claim form that may be used as guides.

4.9.6.5 - Incentive Reward Payment

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

After the complainant has returned the reward claim form with appropriate attachments, the PSC BI unit shall determine the amount of the reward and initiate payment. The reward payment should be disbursed to the complainant from the overpayment money recovered. Payments made under this system are considered income and subject to reporting under Internal Revenue Service tax law. No systems changes to implement these procedures are to be made.

For PSCs, only the AC or MAC shall make IRP payments. The PSC shall provide the necessary documentation to the AC *or MAC* to initiate the IRP payment.

4.9.6.6 - Reward Payment Audit Trail

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI unit shall maintain an audit trail of the disbursed check. The following data shall be included:

- Amount of the disbursed check
- Date issued
- Check number
- Overpayment amount identified
- Overpayment amount recovered
- Social Security number of complainant
- Party the complaint is against

The PSC BI unit shall update the IRP tracking database to reflect disbursement of the reward check to the complainant, and the PSC shall work with the AC *or MAC* via the JOA to disburse the reward check.

4.9.7 - CMS Incentive Reward Winframe Database

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The IRP database was designed to track rewards that could be paid for information about fraud or abuse of the Medicare Trust Fund. Access to the IRP database is through the

Winframe file server located at the CMS data center and is controlled through password and access codes. Cases can be entered into the IRP system by any PSC, or managed care organization contractor, or by the OIG. When the PSC BI unit refers a case to the OIG, for which the complaint is eligible for the IRP, they shall update the IRP system with all available information. The database contains the current status of all Medicare fraud/abuse cases pending reward. Some cases may be closed without a reward, based on final disposition of the case. PSC BI units and CMS ROs have oversight responsibility for this system. The database provides the following information:

- On-demand management reports
- Duplicate complaints submitted for reward
- Audit trail of overpayments recovered as a result of the reward program

The IRP database user instructions are found in PIM Exhibit 5.3.

4.9.8 - Updating the Incentive Reward Database

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall be responsible for updating the incentive reward database on overpayment recovery and reward amounts. PSC BI units shall regularly follow up with the OIG to obtain information on recovery of complaints referred to them that originated from an IRP complainant. The PSC BI units shall follow up on referrals to the OIG when no action is taken within 90 calendar days. The tracking system database shall be updated as information becomes available. Updates shall be entered, at a minimum, on a quarterly basis.

IRP screens may be viewed in PIM Exhibit 5.9

4.10 - Fraud Alerts

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Fraud Alerts are issued when there is a need to advise the PSCs, Carriers, Fiscal Intermediaries, *MACs,* law enforcement, QIOs, and beneficiary communities about an activity that resulted in the filing of inappropriate and potentially false Medicare claims.

The Fraud Alert describes the particular billing, merchandising practice, or activity in enough detail to enable the PSC BI unit to determine whether the practice exists in their jurisdiction.

When *a Fraud Alert is officially issued*, the PSC BI unit shall determine whether the scheme exists within their jurisdiction. *All Fraud Alerts shall be reviewed and reevaluated annually, for at least three years from the date the Fraud Alert was issued, and if necessary, PSC BI units shall take the appropriate actions* to protect the Medicare Trust Fund. Action may include denials, suspensions, overpayment recovery, and/or

conducting of an investigation for case referral to OIG. In each case, the action the PSC BI unit takes shall be based on findings developed independently of the Alert. Once the Alert has been investigated, the results of the investigation shall be reported to the CMS RO SME (i.e., whether the scheme exists in the PSC's jurisdiction) and the steps that were taken to safeguard the Medicare Trust Fund.

4.10.1 - Types of Fraud Alerts

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Below are the various types of Fraud Alerts that are issued:

A. National Medicare Fraud Alert

The most commonly issued Fraud Alert is the National Medicare Fraud Alert (NMFA). (See PIM Exhibit 27 for the NMFA template). NMFAs do not identify specific providers or other entities suspected of committing fraud. They focus on a particular scheme or scam and are intended to serve as a fraud detection lead.

The CO issues an NMFA when a fraudulent or abusive activity is perceived to be, or has the potential for being widespread, i.e., crossing PSC jurisdictions. These Alerts are numbered sequentially. Because CMS and OIG use a comparable numbering system, CMS National Medicare Fraud Alerts are identified as "CMS NMFA," followed by the Alert number appearing in the bottom left-hand corner. OIG Alerts are identified by "OIG," followed by the Alert number appearing in parenthesis in the bottom left-hand corner. The National Medicare Fraud Alert shall be put on the blue CMS fraud stationery. PSCs shall distribute Alerts to all agencies in their jurisdiction within 15 working days of receipt by the PSC BI unit.

Draft National Medicare Fraud Alerts to CO shall be password protected and e-mailed to the CMS CO Director of the Division of Benefit Integrity Management Operations.

An NMFA shall contain the two following disclaimers, in bold print:

Distribution of this Fraud Alert is Limited to the Following Audience:

> Regional offices, program safeguard contractors, Medicare Integrity Program units, quality improvement organizations, Medicaid Fraud Control units, the Office of Inspector General, the Defense Criminal Investigation Service, the Department of Justice, the Federal Bureau of Investigation, U.S. Attorney offices, U.S. Postal Inspectors, the Internal Revenue Service, State surveyors, State Attorneys General, and the State Medicaid program integrity directors.
>
> This Alert is provided for educational and informational purposes only. It is intended to assist interested parties in obtaining additional information concerning potential fraud and to alert affected parties to the nature of the suspected fraud. It is not intended to be used as a basis for denial of claims or any adverse action

against any provider or supplier. Such decisions must be made based on facts developed independent of this Alert.

The NMFA does not include a sanitized version, because it does not identify specific providers or entities. The sharing of NMFAs with individuals or groups that are not on the approved distribution list will be left to the discretion of the PSCs. However, if the PSCs choose to share the NMFAs beyond the approved list, the discovery and detection methodology sections shall not be included. These sections shall be disclosed only to the entities appearing on the audience line of the Fraud Alert.

B. Restricted Medicare Fraud Alert

The CMS issues an RMFA when specific providers are identified as being suspected of engaging in fraudulent or abusive practices or activities. PSC BI units prepare this type of Alert (see PIM Exhibit 28 for the RMFA template) when advising other Medicare carriers, intermediaries, *MACs,* PSCs, QIOs, MFCUs, OIG, DCIS, FBI, or DOJ of a particular provider or providers suspected of fraud. These Alerts are numbered sequentially. Because CMS and OIG use a comparable numbering system, CMS Restricted Medicare Fraud Alerts are identified by "CMS RMFA," followed by the Alert number appearing in the bottom left-hand corner. Distribution is limited to PSCs, *intermediaries, carriers, MACs*, CMS, QIOs, OIG/OI, DCIS, FBI, MFCUs, U.S. Postal Service, IRS, and the Offices of the U.S. Attorney. The CO will issue each PSC *BI unit* one copy of an RMFA along with a sanitized version. Each PSC *BI unit* shall distribute said Alert to the agencies in their jurisdiction for reproduction on the red CMS fraud stationery within 15 working days of receipt by the PSC BI unit.

Draft restricted Medicare Fraud Alerts shall be e-mailed password protected via the secure e-mail system. If problems occur with the secure e-mail system, RMFAs shall be mailed to the following address:

Centers for Medicare & Medicaid Services
OFM/PIG/DBIMO
Mail Stop C3-02-16
7500 Security Blvd.
Baltimore, MD 21244
Attention: Fraud Alert Lead

The envelope shall be marked "personal and confidential" and "do not open in mailroom." All RMFAs shall be password protected when mailed on diskette or CD-ROM. The content of this Alert is not disclosable to the public even under the Freedom of Information Act. Public disclosure of information protected by the Privacy Act has serious legal consequences for the disclosing individual. It is intended solely for the use of those parties appearing on the audience line. It contains the names and other identifying information of provider or suppliers who are suspected of fraud.
A restricted Medicare Fraud Alert shall contain the following disclaimer exactly as below:

THIS ALERT IS CONFIDENTIAL. It is not intended to be used as a basis for the denial of any claim or adverse action against any provider. Such decisions must be based on facts independent of this Alert.

Distribution is limited to the following audience:

Regional offices, program safeguard contractors, quality improvement organizations, Medicaid Fraud Control units, the Office of the Inspector General, the Defense Criminal Investigation Service, the Department of Justice, the Federal Bureau of Investigation, U.S. Attorney offices, U.S. Postal Inspector offices, the Internal Revenue Service, and the State Medicaid Program Integrity Directors.

NOTE: The RMFAs will be distributed to Medicare Integrity Program units on a need to know basis.

C. CMS Central Office Alert

The PSC BI units shall prepare a CO Alert when:

- The PSC BI units need to notify CMS of a scheme that is about to be publicized on the national media

- The case involves patient abuse or a large dollar amount (approximately $1 million or more or potential for widespread abuse), or

- The issues involved are politically sensitive, e.g., congressional hearings are planned to accept testimony on a fraudulent or abusive practice

The Alert shall be prepared and submitted in the same manner as a NMFA but the audience line reads “CO Only.” This Alert shall be addressed to: the CMS CO Division of Benefit Integrity Management Operations (DBIMO) Director, the CO PIG Director, the CO PIG Deputy Director, and the CO Fraud Alert Lead.

D. Program Safeguard Contractor BI Unit Alert

- Initially, this Alert generally is sent to the CO as a draft NMFA or RMFA.

- If CMS reviews the Alert and determines that it does not meet the NMFA or RMFA criteria, CMS will deny clearance and issuance.

- The CMS notifies the PSC BI unit of the Alert denial.

- If the PSC BI unit does not provide CMS with any additional information to justify reconsideration, the denial is final. However, the PSC BI Unit may issue denied Alerts as PSC BI unit Al*erts.

- The PSC BI unit shall provide the CO Fraud Alert lead with a copy of this Alert.

E. Waiver Alerts

On occasion, the OIG waives Medicare exclusions imposed on healthcare providers. Generally, the waiver is granted if the provider is the sole community physician or sole source of essential specialized services in the community.

The CMS' Program Integrity Group will be notified by the OIG of these waivers. Upon receipt of this notification, CMS will issue a Waiver Alert to all PSC BI units. The alert will include a copy of the OIG letter granting the waiver to the provider. The OIG letter may include exceptions to the waiver (e.g., the provider's waiver is limited to certain localities).

Upon receipt of the Waiver Alert, PSC BI units shall provide this information to their respective ACs or *MACs* to ensure that Medicare payments are not denied inappropriately.

Additionally, CMS will post a remark to the Medicare Exclusion Database (MED) indicating that a Waiver Alert has been issued. PSC BI units shall also monitor the MED for consistency.

4.10.2 - Alert Specifications

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

All Alerts drafted shall meet the following criteria:

- The Alert shall be entitled "National Medicare Fraud Alert," "Restricted Medicare Fraud Alert," "CMS CO Alert," or "PSC BI unit Alert."

- It shall include an audience line that indicates the audience that needs to be made aware.

- It shall have a subject line that briefly describes the issue or subject of the Alert, including the provider's UPIN, Tax ID number, and FID case number (if applicable).

- It shall include the source of the information that defines the alleged improper/suspect behavior (e.g., *Medicare General Information, Eligibility, and Entitlement Pub. 100-01; Medicare Benefit Policy Pub. 100-02; Medicare National Coverage Determinations Pub. 100-3; Medicare Claims Processing Pub. 100-04; Program Integrity Manual Pub. 100-08; LCD,* etc.).

- The body of the Alert shall describe the matter in enough detail to enable readers to determine their susceptibility to the activity and what they need to do to protect themselves. It includes diagnosis, Current Procedural Terminology (CPT), and

Healthcare Common Procedure Coding System (HCPCS) codes, the dollar amount involved, the states affected, and applicable policy references, as appropriate.

- It shall include a discovery line that indicates how the PSC BI unit who initiated the Alert discovered the problem. (See note below.) This shall be a clear, detailed explanation that will enable others to determine what to look for in their systems. If a previous Fraud Alert was issued addressing a similar situation, it shall include the Fraud Alert reference.

- It shall include a detection methodology detailing the steps or approaches other PSC BI units can use to determine whether this practice is occurring in their jurisdiction (see note below), including the reports run, the edits used, and the timeframes followed.

- It shall include a status that details the current position of the case (e.g., with OIG or FBI, overpayment identified and amount, etc.).

- It shall include the name and telephone number of a person or organization to be contacted in the event of a complaint or question.

- It shall contain the appropriate disclaimer, depending on the type of Alert. CMS CO Alerts and PSC BI unit Alerts do not need a disclaimer.

NOTE: Do not include the "discovery" and "detection methodology" sections when distributing an Alert to a provider professional organization or other outside group. These sections are disclosable only to ROs, PSCs, *fiscal intermediaries*, *carriers, MACs*, and federal law enforcement agencies. Restricted Alerts shall not be distributed beyond the approved distribution list.

4.10.3 - Editorial Requirements

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall adhere to the following requirements when drafting a Fraud Alert:

- Avoid an emotional writing style such as frequent exclamation points, underlining, and bold type. State the issue in as matter-of-fact a way as possible.

- Avoid generalizing the problem to groups, specialties, or types of providers. Focus on the billing practice or issue.

- Do not state that performance of the activity is fraud, even if the practice does violate Medicare requirements. Couch the message in terms of "alleged," "suspected," "potential," and "possible," fraud, or say it "may be fraud."

- When stating applicable penalties, use “may” (e.g., “may result in exclusion from the Medicare and Medicaid programs”). Do not state that certain penalties will be applied.

- Avoid programmatic jargon or unnecessary terms of art. Use plain English, whenever possible, while remaining technically accurate. If technical terms are necessary, explain them.

Be certain the Alert is technically accurate, and review it prior to submitting a proposed Alert to CMS CO for publication. Consult with RO and OIG, as necessary. Do not sacrifice technical accuracy in the interest of a speedy issuance or writing in plain English.

Issue portions of Alerts in Spanish or other appropriate foreign language if there is a non-English-speaking population that is potentially affected by the scheme, and there are plans to distribute the Alert to such groups.

4.10.4 - Coordination

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Before preparing an Alert, the PSC BI unit shall consult with the PSC network, Primary GTL, Associate GTL, and SME. The PSC BI unit shall determine whether or not a similar Alert has been issued by contacting PSC BI units in contiguous jurisdictions. If so, that Alert shall be used and the name and address of your organization shall be added to the contact section. The PSC BI unit shall forward the draft to CMS Program Integrity Group or the Primary GTL, Associate GTL, and SME for review and clearance. The Program Integrity Group *acknowledges receipt of the draft alert, reviews the draft Alert and when necessary, informs the PSC BI unit that the Program Integrity Group(PIG) needs additional information and/or clarification of certain information within the Alert. All revisions to the Alert by the PSC BI units must be done through track changes and returned to the PIG. As a result of the revisions received by the PIG, the draft Alert will be reevaluated. The PIG will keep the PSC BI unit informed of the progress of the Alert throughout the clearance process. Once a decision has been made, the PIG will notify* the PSC BI unit whether:

- A National Medicare Fraud Alert will be issued

- A Restricted Medicare Fraud Alert will be issued, or

- The Alert should be issued as a PSC BI unit Alert

The CO keeps the PSC BI unit informed of the progress of the Alert throughout the clearance process.

4.10.5 - Distribution of Alerts

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The CMS issues the Alert to the PSCs BI units for further distribution. Approved NMFAs are sent through the electronic mail system (password protected) and approved RMFAs are mailed (password protected diskette, CD ROM). Upon receipt of an approved Alert, the PSC BI unit shall add their name and telephone number to the existing contact information on the Alert. They shall then reproduce the Alert on their own supply of CMS approved stationery. PSC BI units shall distribute the Alert to the entities that appear on the audience line.

4.11 – Fraud Investigation Database Entries

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The Fraud Investigation Database (FID) is a nationwide database of Medicare fraud and abuse investigations, cases, and payment suspensions by the PSC BI unit.

The following agencies/organizations currently have access to the FID:

- Medicare Program Safeguard Contractor *BI units*
- Affiliated Contractor and *Medicare Administrative Contractor* Provider Enrollment units
- CMS
- FBI
- DOJ
- DHHS/OIG
- Medicaid Program Integrity Directors, SURs (State Utilization Review) officials, and Provider Enrollment units
- Medicaid Fraud Control Units
- Other federal and state partners seeking to address program integrity concerns in judicial or state health care programs

4.11.1 - Background

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The FID *captures* information on investigations that have been initiated by the PSC BI unit and on cases that have been referred to law enforcement by the PSC BI unit. The FID also *captures* information on payment suspensions that have been imposed.

Investigations initiated by the PSC BI unit shall be saved in the FID, and contain identifying information on the potential subject of a case. Cases initiated by the PSC BI unit shall contain a summary of the pertinent information on the case referral. At a minimum, the following data shall be included in the case:

- Subject of the case (e.g., physician, hospital, skilled nursing facility, home health agency, comprehensive outpatient rehabilitation facility).

- Allegation information/nature of the scheme.

- Status of the case.

- Disposition of a case (e.g., administrative action, prosecution, exclusion, settlement)..

- Contact information for the PSC BI unit and/or law enforcement.

Payment suspensions shall contain a summary of the pertinent information on the suspension, including date implemented, rebuttal information, and amounts in suspense.

The FID also has monitoring and reporting capabilities, and contains Medicare Fraud Alerts and a Resource Guide, by state, of contacts at PSC BI units, Medicaid Program Integrity Directors and Medicaid Fraud Control Units, and law enforcement agencies.

4.11.1.1 - Information Not Captured in the FID

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Individual complaints (statements alleging improper entitlement), simple overpayment recoveries (not involving potential fraud), complaints that are returned to the AC or *MAC* second-level screening staff (or PSC, if applicable), and medical review abuses shall not be captured in the FID.

4.11.1.2 - Entering OIG Immediate Advisements into the FID

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC shall enter all available information into the FID, as an investigation, concurrent with, or within 15 calendar days after, the “immediate advisement” and shall be converted to a case if the OIG accepts it.

4.11.2 – Investigation, Case, and Suspension Entries

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

It is not appropriate for an OIG or FBI agent, DOJ, or an Assistant United States Attorney (AUSA), to request that a PSC BI unit not enter or update an investigation, case, or payment suspension initiated by the PSC BI unit in the FID, except in rare circumstances. PSC BI units shall inform law enforcement agents making such requests that they are

required by CMS to maintain the FID and that they do not have the discretion to do otherwise. The PSC BI unit shall contact the Primary GTL, Associate GTL, and SME in order to resolve the matter.

However, information regarding law enforcement activities that are, or could be considered to be, of a sensitive nature, including but not limited to, planned search warrants, undercover operations and activities, and executed search warrants, where only some of the search warrants have been executed, shall not be entered into the FID.

4.11.2.1 - Initial Entry Requirements for Investigations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Information entered by the PSC regarding investigations shall capture ongoing work in the PSC BI unit. Investigations are entered when they are reported on the *CMS* ART report.

Investigations initiated by the PSC BI unit shall be entered into the FID within 15 calendar days of the start of the investigation (Investigations are defined in PIM, chapter 4, §4.7). Investigations shall be saved in the FID and shall not be converted to a case until and unless the investigation results in a referral as a case to the OIG or other law enforcement agency. When an investigation is saved, the FID will assign it an investigation number, starting with the letter N. Any complaints that are returned to the AC or the *MAC* second-level screening staff (or PSC, if applicable) shall not be entered into the FID. Such complaints are returned because they pertain to issues other than fraud and abuse.

The minimum initial data entry requirements into the FID for an Investigation shall be (by Tab):

SUBJECT INFORMATION Tab:

- Subject's Name

- Subject's Address (City, State, and Zip Code)

- Subject Type and Subtype

CASE INFORMATION Tab:

- Allegation

- Allegation Source
- Dates of Services (if known)

ACTIONS Tab:

- Actions Taken by: Contractor

- Action Date: [enter the date the investigation was opened]

- Action Narrative: [enter brief statement on the investigation]

- Action: Under Investigation (for PSC BI unit initiated investigations)

CONTACTS Tab:

[Confirm contact information is accurate]

There are no mandatory update requirements for investigations, but the PSC BI unit shall enter updates as necessary. *If* the PSC BI unit *adds* information during the investigation phase, *the information* shall still be saved in FID as an investigation.

4.11.2.2 – Initial Entry Requirements for Cases

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Once the PSC BI unit has referred a case to the OIG or other law enforcement agency, the investigation shall then be saved as a Case within 15 days of referral. The investigation actually converts to a FID case.

4.11.2.3 – Initial Entry Requirements for Payment Suspension

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC shall enter information *on payment suspensions* into the FID Suspension Module no later than the effective date of the suspension.

4.11.2.4 – Update Requirements for Investigations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

There are no mandatory update requirements for investigations, but the PSC BI unit shall enter updates as necessary. Should the PSC BI unit add information during the investigation phase, it shall still be saved in FID as an investigation.

4.11.2.5 - Update Requirements for Cases

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

For cases referred to the OIG, the FBI, or other law enforcement agency, updates to the FID case shall be made at least every 3 months (1 month is a maximum of 31 days). If problems are encountered which *interfere with* the PSC BI units' ability to get updated information, this shall be discussed with the appropriate Primary GTL, Associate GTL, and SME.

As applicable, the following tabs/sections shall be updated:

- Referrals accepted by OIG or FBI are assigned a case number by the OIG or FBI. It shall be the responsibility of the PSC BI unit to obtain and enter the case number into the FID Case Information tab;

- The Case Narrative section in the FID Case Information tab shall clearly identify the alleged fraudulent activity, all investigation actions, and referral activities performed on the case by the PSC BI unit. The sooner comprehensive case information is entered into FID, the more efficiently other PSCs, CMS, Medicaid, and law enforcement agencies can react to the case and perform related trend-data analysis;

- The PSC BI unit shall enter updated summary information in the FID Actions tab after the case is referred to the OIG/FBI. The status of the case and, when appropriate, actions taken by law enforcement shall be entered into the FID. If the PSC BI unit is not able to obtain status on cases referred to and accepted by law enforcement, this shall be brought to the attention of the appropriate Primary GTL, Associate GTL, and SME. All corrective and/or administrative actions taken by the AC, *MAC, or* PSC shall be entered into the FID;

- Contact with the FBI or an AUSA regarding their actions on a case;

- Capturing and documenting subsequent law enforcement referrals (e.g., OIG declines case, PSC BI unit refers case to FBI, FBI accepts case);

- Keeping apprised of MR/provider audit and reimbursement actions if they are taking actions on a case;

- Updating the amount being withheld, denied, or paid;

- Entering information on convictions/sentences; and/or,

- Adding to the case narrative section in the Case Information tab, to incorporate any updated information summarized in the Actions tab.

The PSC BI unit shall document in the FID any consultations with law enforcement as well as administrative actions and associated monetary assessments by the PSC BI unit or law enforcement.

4.11.2.7 - OIG Non-Response to or Declination of Case Referral

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

As per instructions found in PIM, Chapter 4, §4.18.1, if the PSC BI unit does not *receive a response* from the OIG within the first 90 days following referral, and if repeated attempts by the PSC BI unit to *determine* the status of the case are unsuccessful, the PSC BI unit shall then refer the case first to the FBI, and if FBI declines the case, to any other law enforcement agency with interest in the case. If this subsequent referral to the FBI or any other investigative agency is not acted upon within 45 days, the PSC BI unit shall follow up with the FBI or other investigative agency. Subsequent to follow-up, the PSC BI unit may close the case in the FID if it is still not acted upon by the FBI or other law enforcement agency, but shall continue to enter any actions that it takes, including administrative actions. For FID tracking purposes, the PSC BI unit shall make any additional entries, based upon administrative or other actions taken, or, in the alternative, shall reopen the same FID case at some future time if the OIG, FBI, or other law enforcement agency accepts the case.

If the OIG formally declines a referral and does not itself refer the case to the FBI, the PSC BI unit shall refer the case first to the FBI and then to another law enforcement agency if the FBI declines the case. However, when a case is referred to FBI in this situation, it shall be considered an update to the existing FID case, reflecting a subsequent action taken on the case, and not a new FID case. That is, subsequent referrals of the same case to other law enforcement agencies shall not be counted as new case entries in the FID, nor are they counted for workload purposes as new referrals to law enforcement.

4.11.2.8 – Closing Investigations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Investigations shall be closed when they are no longer reported as an investigation on CMS analysis, reporting and tracking (ART) (refer to §4.7.2 for a definition of when to close an investigation). The investigation that does not result in referral of a case shall be closed by entering the following action in the ACTIONS Tab in order to indicate that the investigation has been closed:

ACTIONS Tab:

- Action Taken by: Contractor

- Action: Investigation Closed

The PSC BI unit shall also enter administrative actions, if any, it has taken as part of disposition of the investigation.

4.11.2.9 – Closing Cases

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

An active FID case shall be closed when no further action will be required of the PSC or Medicare contractor BI unit by law enforcement agency(ies) working the case and when the law enforcement agency(ies) has ended all its activity on the case; and when all necessary administrative actions have been finalized (i.e., when the calculated overpayment has been referred to the AC *or MAC* for recoupment). Note that after a case is closed, it can still be updated to reflect any additional activity that takes place (i.e., recoupment of the overpayment by the AC *or MAC*).

4.11.2.11 - Duplicate Investigations, Cases, or Suspensions

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

A duplicate investigation, case, or suspension exists when any given PSC BI unit inadvertently enters a provider, supplier, or beneficiary as the subject of an investigation, case, or payment suspension more than once, absent different allegations or other differentiating criteria requiring a separate investigation, case, or suspension entry.

For investigations, cases, and suspensions, it shall not be considered a duplicate investigation, case, or suspension if multiple PSC BI units enter investigations, cases, or suspensions for the same provider as the subject of an investigation, case, or suspension. These investigations, cases, and suspensions, however, shall reflect a coordinated effort by all PSC BI units involved and investigating the provider. Case numbers shall be referenced in the Subject Information tab, Related FID Case No. field, and the case description summaries shall reflect this coordination. The FID now has the capability of cross-checking for related cases.

If a new investigation or case is initiated on a provider that was already the subject of a closed investigation or case, a new investigation or case shall be opened. The closed investigation or case, however, shall be mentioned in the Case Narrative screen in the Case Information Tab and cross-referenced to the old investigation or FID case number.

The target, whether entity or individual, shall be entered as the subject of the investigation or case. Any and all related providers, suppliers, beneficiaries, etc., who are in any way affiliated with the subject of the case, shall be identified under “AKAs, DBAs, and Affiliates.” However, if these individuals are the primary subjects/targets of the investigation or case and independent investigations or cases are made against them, then individual investigations or cases shall be established in the FID.

If a new payment suspension has been imposed on a provider that was already the subject of an earlier payment suspension, a new payment suspension shall be entered into the FID. The prior (now inactive) suspension, however, shall be cross-referenced in the Contacts/Narrative Information tab - Suspension Narrative section.

The PSC BI units shall check for potential duplicate entries of investigations, cases, or suspensions.

4.11.2.12 – Deleting Investigations, Cases, or Suspensions

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Investigations, cases, or suspensions can be deleted from the FID only by users with the “File Manager” (system administrator) designation. As applicable and necessary, the Primary GTL, Associate GTL, and SME will contact and discuss with the PSC BI unit the need to correct and/or delete an investigation, a case, or suspension from the database. In the event that a PSC decides that an investigation, a case, or suspension should be

deleted from the FID, the investigation number, case number, or suspension number shall be forwarded to the FID mailbox at FID@cms.hhs.gov.

4.11.3.1 - Access

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

If PSC BI units, and others eligible to access the FID have never applied for access to the FID system and require authorization, an "Application for Access to CMS Computer Systems" shall be completed, submitted, and approved.

This form may be acquired from http://www.cms.hhs.gov/mdcn/access.pdf. It shall be submitted to the appropriate RACF (Resource Access Control Facility) Group Administrator for all CMS central and regional offices, or to the Primary GTL for PSCs or to the CMS Division of Benefit Integrity Management Operations for all law enforcement personnel or other users.

The CMS Remote Access Guide can be found at the following website: http://www.cms.hhs.gov/mdcn/cmsremoteaccessguide.pdf.

For those individuals who have received prior authorization, but are experiencing authorization lapses or password problems, the same contacts referenced above shall be contacted. Internet access problems shall be directed to the CMS IT Service Desk, at (410) 786-2580 or 1-800-562-1963.

4.11.3.2 - The Fraud Investigation Database User's Group

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Membership in the FID User's Group is voluntary and open to all Users. The group discusses proposed enhancements, upgrades, current issues, matters of interest to users, etc. Anyone interested in joining the group can send an email to the FID mailbox: FID@cms.hhs.gov

Notice of programming changes in the FID (e.g., enhancements, upgrades, changes to entry requirements) shall be issued by the FID User's Group, and disseminated as widely as possible. PSC BI units shall refer to FID User's Group minutes for entry instructions. Programming changes are also communicated via News Items posted in the FID.

4.11.3.3 – Designated PSC BI Unit Staff and the Fraud Investigation Database

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The designated PSC BI unit staff receive training on how to input and maintain cases in the FID. The intent is to use these staff members as FID experts and points of contact for questions and comments on the FID. They shall be responsive to FID questions from PSC BI units and law enforcement personnel within their jurisdiction.

Designated PSC BI unit staff shall serve as a resource to CMS on the FID, including FID training.

Designated staff at each PSC BI unit shall be responsible for sharing FID information and analysis (e.g., FID system reports) with the PSC BI manager and BI staff. If the designated PSC BI unit staff detects any inaccuracies or discrepancies in cases entered by their PSC BI unit, they shall notify the PSC BI manager.

4.11.3.4 - The Fraud Investigation Database Mailbox

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Questions, comments, or suggestions *regarding* the FID *may be sent via* the FID *to* FID@cms.hhs.gov

4.12.2 - Harkin Grantee Tracking System Instructions

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The AC or *MAC* second-level screening staff shall be responsible for collecting, tracking, and reporting the administrative and monetary results of fraud and abuse complaints generated by the Harkin Grantees or Senior Medicare Patrol state projects, including those complaints referred to the PSC BI unit. The AC or *MAC* second-level screening staff shall develop aggregate reports available to the Harkin Grantees or Senior Medicare Patrol state project coordinators every 6 months.

The Harkin Grantees or Senior Medicare Patrol State/local contact information is available at http://www.aoa.gov/smp/index.asp

4.12.3 - System Access to Metaframe and Data Collection

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The Harkin Grantees Tracking System migrated from the Winframe to the Metaframe server. Access the Metaframe system as follows:

Download the new Citrix Client and upgrade. Download the Client software: http://download2.citrix.com/files/en/products/client/ica/current/ica32.exe

Each AC and *MAC* shall designate a person in the second-level screening staff to input the complaint into the HGTS database located on the Metaframe system. These designees shall enter data on a continuous basis related to complaints generated by the Harkin Grantees or Senior Medicare Patrol state projects.

The Harkin Grantees or Senior Medicare Patrol will report their complaints according to their usual procedure, using the model complaint form (PIM Exhibit 32).

Upon receiving Harkin Grantees or Senior Medicare Patrol complaints, the AC or *MAC* second-level screening staff shall enter the following information into the Metaframe database fields.

- Project number
- Date of Report
- Provider Number
- Provider Name
- Provider City
- Provider State

- AC or *MAC* Number
- Overpayment Identified
- Overpayment Recovered
- Action Taken
- Further Explanation

If the PSC BI unit completes the complaint review, they shall provide the above information, as applicable, to the AC or *MAC* second-level screening staff for input.

4.12.4 - Data Dissemination/Aggregate Report

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The AC or *MAC* second-level screening staff shall compile information in the database into an aggregate report. The AC or *MAC* shall distribute the aggregate report to the Harkin Grantees or Senior Medicare Patrol state project coordinators every 6 months. Aggregate reports shall be distributed by the second week of July (covering January - June data) and the second week of January (covering July - December data).

The January through June/July through December report cycle shall be continuous until further instruction.

The AC's and *MAC's* second-level screening staff shall forward copies of the aggregate reports to the CMS CO Director of the Division of Benefit Integrity Management Operations.

4.13 - Administrative Relief from Benefit Integrity Unit Review in the Presence of a Disaster

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

During a disaster, whether man-made or natural, the PSC BI unit shall continue every effort to identify cases of potential fraud. Therefore, if the PSC BI unit suspects fraud of a provider who cannot furnish medical records in a timely manner due to a disaster, the PSC BI unit shall ensure that the provider is not attempting to harm the Medicare Trust Fund by taking 6 months or more to furnish medical records. *The* PSC BI unit shall request and review verification documentation in all instances where fraud is suspected.

In the case of complete destruction of medical records/documentations where backup records exist, PSC BI units shall accept reproduced medical records from microfiched, microfilmed, or optical disk systems that may be available in larger facilities, in lieu of the original document. In the case of complete destruction of medical records where no backup records exist, PSC BI units shall instruct providers to reconstruct the records as *completely as possible* with whatever original records can be salvaged. Providers should

note on the face sheet of the completely or partially reconstructed medical record: “This record was reconstructed because of disaster.”

4.14 - Provider Contacts by the Program Safeguard Contractor Benefit Integrity Unit

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

A PSC BI unit may determine that the resolution of an investigation does not warrant referral for criminal, CMP, or sanction, and that an educational meeting with the provider is more appropriate. The PSC BI unit shall inform the provider of the questionable or improper practices, the correct procedure to be followed, and the fact that continuation of the improper practice may result in administrative sanctions. The PSC BI unit shall document contacts and/or warnings with written reports and correspondence and place them in the investigation file. If the improper practices continue, the PSC BI unit shall consult with the OIG/OI contact person regarding sanction action.

If the provider continues aberrant billing practices during the period for which it is being investigated for possible sanction, the PSC BI unit shall initiate the adjustment of payments accordingly with the AC or *MAC*. After meeting with a provider, the PSC shall prepare a detailed report for the investigation file, and shall forward a copy to OIG/OI along with a case referral, if requested. The report shall include the information in A, B, and C below.

A. Background of Provider (Specialty)

PSC BI units shall include a list of all enterprises in which the subject had affiliations, the states where the provider is licensed, all past complaints, and all prior educational contacts/notices.

B. Total Medicare Earnings

PSC BI units shall include a report of the total Medicare earnings for the past 12 months, as well as total dollars for assigned and non-assigned claims in that period in the case file.

The report shall include the following:

- Earnings for the procedures or services in question
- Frequency of billing for these procedures/services
- Total number of claims submitted for these procedures/services

C. Extent of Audit Performed

The PSC BI units shall include:

- A report of your audit process and findings
- Overpayment identified
- Recommendation(s)

D. Report of Meeting

The PSC BI units include:

- Minutes from the meeting describing the problems and/or aberrancies discussed with the provider and the education provided to the provider to correct those problems, and
- Copies of educational materials given to the provider before, during, or subsequent to the meeting.

4.16 – AC, *MAC,* and PSC Coordination on Voluntary Refunds

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Voluntary refund checks payable to the Medicare program shall not be returned, regardless of the amount of the refund. The PSC BI unit shall communicate with the AC or *MAC* staff responsible for processing voluntary refunds to obtain information on voluntary refund checks received. The PSC BI unit shall perform an investigation on any voluntary refunds where there is suspicion of inappropriate payment or if a provider is under an active investigation.

Should the PSC BI unit receive a voluntary refund check in error, the PSC shall coordinate the transfer of voluntary refund checks to the AC *or MAC* through the JOA.

The ACs and *MACs* shall refer to the Financial Management Manual for instructions on processing and reporting unsolicited/voluntary refunds received from providers/physicians/suppliers.

Through the JOA, PSCs shall establish a mechanism whereby the AC *or MAC* notifies the PSC on a regular basis of all voluntary refunds received by the AC *or MAC*. PSCs *or* ACs and *PSCs or MACs* shall send one letter annually (calendar year) to any provider that submits a voluntary refund during that calendar year, advising the provider of the following:

> The acceptance of a voluntary refund in no way affects or limits the rights of the Federal Government or any of its agencies or agents to pursue any appropriate criminal, civil, or administrative remedies arising from or relating to these or any other claims.

The PSCs and ACs *or the PSCs and MACs* shall work out in the JOA whether the PSC *or*

AC *and the PSC or MAC* sends the above language. The ACs *and MACs* may send the language above on a voluntary refund acknowledgement letter or on a Remittance Advice if this capability exists.

The PSC BI units shall refer to chapter 4, §4.4.1G and H, for law enforcement requests for voluntary refund information.

4.18.1 - Referral of Cases to the Office of the Inspector General/Office of Investigations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall identify cases of suspected fraud and shall make referrals of all such cases to the OIG/OI, regardless of dollar thresholds or subject matter. Matters shall be referred when the PSC BI unit has documented allegations, including but not limited to: a provider, beneficiary, supplier, or other subject, a) engaged in a pattern of improper billing, b) submitted improper claims with suspected knowledge of their falsity, or c) submitted improper claims with reckless disregard or deliberate ignorance of their truth or falsity. In cases where providers' employees submit complaints, such cases shall be forwarded to the OIG immediately.

When a case has been referred to OIG/OI, OIG/OI has 90 calendar days to accept the referral, refer the case to the DOJ (for example, the FBI, AUSAs, etc.), or to reject the case. If the PSC BI unit does *not receive a response* from OIG/OI within the first 90 calendar days following referral, and repeated attempts by the PSC BI unit to find out the status of the case are unsuccessful, the PSC BI unit shall contact the FBI (if the FBI does not have the case referral, the PSC BI unit shall refer the case to them) and/or refer the case to any other investigative agency with interest in the case. The PSC BI unit shall follow up on this second referral to the FBI and any other investigative agency within 45 calendar days. Refer to the FID section of the PIM for the requirements on entering and updating referrals in the FID. If OIG/OI or other law enforcement agencies will not give a definite answer, *the PSC shall* contact the Primary GTL, Associate GTL, and SME for assistance. If OIG/OI or other law enforcement agencies do not accept the case or are still unwilling to render a decision on the case, even after the intercession of the Primary GTL/Associate GTL/ SME, PSC BI units shall proceed with action to ensure the integrity of the Medicare Trust Fund (e.g., PSC BI units shall discuss it with the AUSA and/or the OIG prior to taking administrative action).

The OIG/OI will usually exercise one or more of the following options when deciding whether to accept a case:

- Conduct a criminal and/or civil investigation

- Refer the case back to the PSC BI unit for administrative action/recovery of overpayment with no further investigation

- Refer the case back to the PSC BI unit for administrative action/recoupment of overpayment after conducting an investigation or after consulting with the appropriate AUSA's office

- Refer the case back to the PSC BI unit for administrative action/recoupment of overpayment after the AUSA's office has declined prosecution

- Refer the case to another law enforcement agency for investigation

Where OIG/OI conducts an investigation, OIG/OI will usually initiate ongoing consultation and communication with the PSC BI unit to establish evidence (i.e., data summaries, statements, bulletins) that a statutory violation has occurred.

In addition to referral of such cases to the OIG, PSC BI units shall also identify and take additional corrective action and prevent future improper payment (for example, by placing the provider's or supplier's claims on prepayment review). In every instance, whether or not the investigation is a potential case and law enforcement referral, the first priority is to minimize the potential loss to the Medicare Trust Fund and to protect Medicare beneficiaries from any potential adverse effect. Appropriate action varies from case to case. In one instance, it may be appropriate to suspend payment pending further development of the case. In another instance, suspending payment may alert the provider to detection of the fraudulent activity and undermine a covert operation already underway, or being planned, by federal law enforcement. PSC BI units shall continue to monitor the need for administrative action prior to the elapsing of the 90 days and thereafter, and consult with OIG or other law enforcement agencies before taking such measures. The OIG may provide the PSC BI unit with information that shall be considered in determining what corrective action should be taken. If law enforcement is unwilling to render a decision on administrative action or advises the PSC BI unit against taking administrative action, the PSC shall contact the Primary GTL, Associate GTL, and SME will decide whether or not to take administrative action.

The PSC BI unit shall alert and coordinate with OIG/OI, FBI, the civil and criminal divisions in the U.S. Attorney's Office, and the RO, of contemplated suspensions, denials, and overpayment recoveries where there is reliable evidence of fraud and a referral pending with the OIG/OI or FBI, or a case pending in a U.S. Attorney's Office that may be known or unknown to the PSC BI unit.

If the case is the focus of a national investigation, PSC BI units shall not take action without first consulting with the Primary GTL, Associate GTL, and SME and the agency that has the lead for the investigation.

4.18.1.2 - Immediate Advisements to the OIG/OI

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI unit shall immediately advise the OIG/OI through a telephone communication to the special agent in charge (SAC) or assistant special agent in charge (ASAC) and maintain internal documentation on these advisements when it receives allegations with one or more of the following characteristics:

- Indications of PSC, AC, or *MAC* employee fraud.

- Cases involving an informant that is an employee or former employee of the suspect physician or supplier.

- Involvement of providers who have prior convictions for defrauding Medicare or who are currently the subject of an OIG fraud investigation.

- Situations involving the subjects of current program investigations.

- Multiple carriers involved with any one provider (OIFO coordinates activities with all involved carriers).

- Cases with, or likely to get, widespread publicity or involving sensitive issues.

- Allegations of kickbacks or bribes.

- Allegations of a crime by a federal employee.

- Indications that organized crime may be involved.

- Indications of fraud by a third-party insurer that is primary to Medicare.

For OIG Hotline complaints with one or more of the above characteristics, the PSC BI unit shall promptly telephone the SAC or ASAC and describe the nature of the allegations. This communication ensures that the SAC or ASAC knows about the allegations from the OIG Hotline and gives the PSC BI unit an opportunity to request further direction (if such direction has not already been given) from the SAC. In addition, the PSC BI unit shall document the telephone conversation through a written communication (e.g., an e-mail or letter) to the SAC or ASAC. This approach ensures that Immediate Advisements are timely and provides an audit trail for the BI unit.

The PSC BI units shall not expend resources attempting to investigate the allegation until so directed by CMS and/or the OIG. For example, if a PSC BI unit receives an allegation of kickbacks, the PSC BI unit shall immediately advise the OIG of the allegation, but shall not initiate an independent PSC BI unit query until requested to do so by the OIG and guidance on the parameters of the query are provided by the OIG. If the query

requested by the OIG becomes costly or requires major resources or is outside the scope of the normal law enforcement requests (e.g., requesting the PSC BI units to conduct an interview for the development of a kickback case), the PSCs shall discuss this with the GTL, Associate GTL, and SME before fulfilling the OIG query request.

When an "immediate advisement" is required, all available documentation received with the allegation shall be forwarded to the OIG, unless otherwise directed by OIG. However, the initial forwarding of the applicable information does not equate to the PSC BI unit completing the full referral package as defined in the PIM (see PIM, Exhibit 16.1), and does not equate to a case referral to law enforcement.

Refer to the FID section of the PIM for entering immediate advisements into the FID.

4.18.1.3 - Program Safeguard Contractor BI Unit Actions When Cases Are Referred to and Accepted by OIG/OI

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Even though OIG/OI or another law enforcement agency has accepted a case, the PSC BI unit *shall* continue to monitor and document the suspect provider's activities. Additional complaints or other information received shall be immediately forwarded to the appropriate agency. Also, PSC BI units may still initiate action to suspend payments, deny payments, or to recoup overpayments.

4.18.1.3.1 - Suspension

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

If payment has not been suspended before OIG/OI accepts a case, PSC BI units shall discuss suspending payments with OIG/OI where there is reliable and substantive evidence that overpayments have been made and are likely to continue. Where OIG/OI disagrees with the suspension on the grounds that it will undermine their law enforcement action and there is disagreement, PSC BI units shall discuss the matter with their designated SME. The SME will then decide, after consulting with OIG/OI, whether the PSC BI unit should proceed with the suspension. Suspension of payment should not be delayed in order to increase an overpayment amount in an effort to make the case more attractive to law enforcement.

Continuing to pay claims submitted by a suspect provider for this purpose is not an acceptable reason for not suspending payment.

The PSC BI units shall refer to PIM, chapter 3, §3.9ff for suspension of payment instructions.

A. Record of Suspended Payments Regarding Providers Involved in Litigation

The PSC BI units shall provide OIG/OI with current information, as requested, regarding total payments due providers on monies that are being withheld because those cases are

being referred for fraud prosecution. (The OIG/OI sends notification of which potential fraud cases have been referred for prosecution.) These monies represent potential assets, against which offset is made to settle overpayments or to satisfy penalties in any civil action brought by the government. The total amount of withheld payments is also pertinent to any determination by the DOJ whether civil fraud prosecution action is pursued or a negotiated settlement attempted.

4.18.1.3.2 - Denial of Payments for Cases Referred to and Accepted by OIG/OI

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Where it is clear that the provider has not furnished the item or services, denial is the appropriate action. (See PIM Exhibit 14.) Before recommending denying payments, PSCs consult with their Primary GTL, Associate GTL, and SME.

4.18.1.3.3 - Recoupment of Overpayments

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall seek to initiate recoupment of overpayments whenever there is a determination that Medicare has erroneously paid. Once an overpayment has been determined, the statute and regulations require that the overpayment be recovered, especially if the overpayment is not related to the matter that was referred to law enforcement (see PIM, chapter 3, §3.8ff). The ACs *and MACs* shall perform recoupment of all overpayments including sending the demand letter.

4.18.1.4 - OIG/OI Case Summary and Referral

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units should use the following format when preparing summaries for referral to OIG/OI including where additional civil, criminal, Civil Monetary Penalty Law (CMPL), or sanctions action appears appropriate. They shall forward two copies of the referral and fact sheet to the OIG, and shall retain a copy of the summary in the case file.

A Case Referral Fact Sheet Format can be found in PIM Exhibit 16.1.
A Case Summary Format can be found in PIM Exhibit 16.2.

4.18.1.5.1 - Continue to Monitor Provider and Document Case File

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall not close a case simply because it is not accepted by OIG/OI. Since the subject is likely to continue to demonstrate a pattern of fraudulent activity, they shall continue to monitor the situation and to document the file, noting all instances of suspected fraudulent activity, complaints received, actions taken, etc. This will strengthen the case if it is necessary to take further administrative action or there is a wish to resubmit the case to OIG/OI at a later date. If PSC BI units do resubmit the case to OIG/OI, they shall highlight the additional information collected and the increased amount of money involved.

4.18.1.5.2 - Take Administrative Action on Cases Referred to and Refused by OIG/OI

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units take immediate action to implement appropriate administrative remedies, including the suspension or denial of payments, and the recovery of overpayments (see PIM, chapter 3, §3.8ff). Because the case has been rejected by law enforcement, PSCs shall consult with the Primary GTL, Associate GTL, and SME concerning the imposition of suspension. They pursue administrative and/or civil sanctions by OIG where law enforcement has declined a case.

A. Denial/Referral Action for Erroneous Payment(s), Cases Not Meeting the Referral Threshold

Many instances of erroneous payments cannot be attributed to fraudulent intent. There will also be cases where there is apparent fraud, but the case has been refused by law enforcement. Where there is a single claim, deny the claim and collect the overpayment. Where there are multiple instances, deny the claims, collect the overpayment, and warn the provider. PSC BI units shall refer the provider, as appropriate, to provider relations, medical review, audit, etc.

4.18.1.5.3 - Refer to Other Law Enforcement Agencies

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

If the OIG/OI declines a case that the PSC BI unit believes has merit, the PSC BI unit may refer the case to other law enforcement agencies, such as the FBI, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), RRB/OIG, and/or the MFCU.

The PSC BI units should recommend administrative and/or civil sanctions (including exclusions) to the OIG where law enforcement has declined the case.

4.18.2 - Referral to State Agencies or Other Organizations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall refer instances of apparent unethical or improper practices or unprofessional conduct to state licensing authorities, medical boards, the QIO, or professional societies for review and possible disciplinary action. If a case requires immediate attention, they shall refer it directly to the state licensing agency or medical society and send a copy of the referral to the QIO.

Some state agencies may have authority to terminate, sanction, or prosecute under state law. It may be appropriate to refer providers to the state licensing agency, to the MFCU, or to another administrative agency that is willing and able to sanction providers that either bill improperly or mistreat their patients (see PIM, chapter 4, §4.18.1.5.3 and §4.19ff). This option is strongly recommended in instances where federal law enforcement is not interested in the case.

In each state there is a Medicare survey and certification agency. It is typically within the Department of Health. The survey agency has a contract with CMS to survey and certify institutional providers as meeting or not meeting applicable Medicare health and safety requirements, called Conditions of Participation. Providers not meeting these requirements are subject to a variety of adverse actions, ranging from bans on new admissions to termination of their provider agreements. These administrative sanctions are imposed by the RO, typically after an onsite survey by the survey agency.

Ordinarily, PSC BI units do not refer isolated instances of questionable professional conduct to medical or other professional societies and state licensing boards. However, in flagrant cases, or where there is a pattern of questionable practices, a referral is warranted. The MR and BI units shall confer before such referrals, to avoid duplicate referrals. There is no need to compile sufficient weight of evidence so that a conclusive determination of misconduct is made prior to the referral. Rather, PSC BI units ascertain the probability of misconduct, gather available information, and leave any further investigation, review, and disciplinary action to the appropriate professional society or state board. Consultation and agreement between the MR and BI unit shall precede any referral to these agencies.

The PSC shall work closely with their Primary GTLs, Associate GTLs, and SME on these referrals.

Concurrently, PSC BI units shall notify OIG/OI of any referral to medical or other professional societies and state licensing boards in cases involving unethical or unprofessional conduct. They shall include with the notification to OIG/OI copies of all materials referred to the society or board. PSC BI units shall send OIG/OI a follow-up report on significant developments. They shall notify OIG/OI about possible abuse situations when it appears that a harmful medical practice or a sanctionable practice is occurring or has occurred.

Notice of suspension should also be given to the Medicaid SURs since a significant percent of Medicare beneficiaries are eligible for both Medicare and Medicaid and Medicaid is paying co-payments.

4.18.3 - Referral to Quality Improvement Organizations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Communication with the QIO is essential to discuss the potential impact of efforts to prevent abuse as well as efforts to ensure quality and access. More specifically, CMS expects dialogue between PSCs and the QIO to:

- Ensure that an *LCD* does not set up obstacles to appropriate care
- Articulate the program safeguard concerns or issues related to QIO activities
- Be aware of QIO initiatives (e.g., a QIO project to encourage Medicare beneficiaries to get eye exams), so they do not observe an increase in utilization and label it overutilization

The PSCs should continue exchanging additional information such as data analysis methods, data presentation methods, and successful ways to interact with providers to change behavior. This includes special projects that PSCs and the QIO have determined to be mutually beneficial.

It is essential that the PSC manager maintain an ongoing dialogue with his/her counterpart(s) at other PSCs, particularly in contiguous states. This ensures that a comprehensive investigation is initiated in a timely manner and prevents possible duplication of investigation efforts.

The PSCs should maintain an ongoing dialogue with the QIOs. Intermediaries *or MACs* may make referrals to the QIO for review of inpatient claims when outpatient claims reveal a problem provider. If the PSC refers a provider to the state licensing agency or medical society, i.e., those referrals that need immediate response from the state licensing agency, it should also send a copy of the referral to the QIO. Also, PSCs shall notify the QIO on utilization and quality issues for Part A providers and physicians that are suspected of fraud and of referrals to OIG/OI.

The PSC shall coordinate the review of Part A acute care inpatient hospital claims and long term care hospital PPS claims (i.e., long term acute care, not SNFs) for benefit integrity purposes with the QIO. The PSC shall follow the definition of acute care inpatient prospective payment system (PPS) hospital found in PIM Chapter 1, §1.1.2 (http://www.cms.gov/manuals/108_pim/pim83c01.pdf). If the PSC investigation indicates a need to review Part A acute care inpatient PPS hospital medical records or long term care hospital PPS claim medical records, the PSC shall request the medical records directly from the provider and have them sent directly to the PSC. Upon receipt of the records, the PSC shall perform a billing and document review of the medical

record. The PSC shall also review the medical records for medical necessity, as well as, any indications of potential fraud and abuse. The PSC shall not initiate any payment determination, provider education, overpayment calculation, or overpayment request based on these medical records. QIOs will conduct or initiate these activities as appropriate.

Following PSC review of the Part A acute care inpatient PPS hospital claims or long term care hospital PPS claims and medical records, if the PSC determines that no potential fraud and abuse has been committed, or if the PSC determines that potential fraud and abuse is likely but law enforcement rejects the case, the PSC shall refer the provider and medical records back to the QIO for further medical review, provider education, or the initiation of overpayment calculation, payment determination, and overpayment request.

If the PSC wants to follow up with the AC *or MAC* on such referrals concerning the overpayments, the PSC should include this in the JOA.

If after the PSC reviews the Part A acute care inpatient PPS hospital claims or long term care hospital PPS claims and medical records, the PSC determines that potential fraud and abuse is likely, the PSC shall coordinate the case with law enforcement (per Law Enforcement Memorandum of Understanding). If law enforcement accepts the case, law enforcement may then coordinate directly with the QIO for any further medical review.

The PSC shall not involve the QIO in reviews at other types of hospitals.

4.19 - Administrative Sanctions

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The term “sanctions” represents the full range of administrative remedies and actions available to deal with questionable, improper, or abusive practices of practitioners, providers, and suppliers under the Medicare and Medicaid programs or any state health care programs as defined under §1128(h) of the Act. There are two purposes for these sanctions. First, they are designed to be remedial, to ensure that questionable, improper, or abusive practices are dealt with appropriately. Practitioners, providers, and suppliers are encouraged to correct their behavior and operate in accordance with program policies and procedures. Second, the sanctions are designed to protect the programs by ensuring that improper payments are identified and recovered and that future improper payments are not made.

The primary focus of this section is sanctions authorized in §1128 and §1128A of the Act (exclusions and CMPs). Other, less severe administrative remedies may precede the more punitive sanctions affecting participation in the programs. The corrective actions PSCs, ACs, and *MACs* shall initially consider are:

- Provider education and warnings
- Revocation of assignment privileges

- Suspension of payments (refer to PIM, chapter 3, §3.9ff)

- Recovery of overpayments (refer to PIM, chapter 3, §3.8ff)

- Referral of situations to state licensing boards or medical/professional societies

4.19.1 - The Program Safeguard Contractor's, *Affiliated Contractor's,* and Medicare *Administrative* Contractor's Role

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The AC *and MAC* shall be responsible for:

- Ensuring that no payments are made to provider/suppliers for a salaried individual who is excluded from the program. OIG, as it becomes aware of such employment situations, notifies providers that payment for services furnished to Medicare patients by the individual is prohibited and that any costs (salary, fringe benefits, etc.) submitted to Medicare for services furnished by the individual will not be paid. A copy of this notice is sent to the PSC BI unit and to the appropriate RO.

The PSC and the AC *and the PSC and the MAC* shall work out the following in their JOA:

- Furnishing any available information to the OIG/OI with respect to providers/suppliers requesting reinstatement.

- Reporting all instances where an excluded provider/supplier submits claims for which payment may not be made after the effective date of the exclusion.

The PSC BI unit shall also be responsible for:

- Contacting OIG/OI when it determines that an administrative sanction against an abusive provider/supplier is appropriate.

- Providing OIG/OI with appropriate documentation in proposed administrative sanction cases.

4.19.2 - Authority to Exclude Practitioners, Providers, and Suppliers of Services

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Section 1128 of the Act provides the Secretary of DHHS the authority to exclude various health care providers, individuals, and businesses from receiving payment for services that would otherwise be payable under Medicare, Medicaid, and all federal health care programs. This authority has been delegated to the OIG.

When an exclusion is imposed, no payment is made to anyone for any items or services in any capacity (other than an emergency item or service provided by an individual who does not routinely provide emergency health care items or services) furnished, ordered, or prescribed by an excluded party under the Medicare, Medicaid, and all federal health care programs. In addition, no payment is made to any business or facility, e.g., a hospital, that submits claims for payment of items or services provided, ordered, prescribed, or referred by an excluded party.

The OIG also has the authority under §1128(b)(6) of the Act to exclude from coverage items and services furnished by practitioners, providers, or other suppliers of health care services who have engaged in certain forms of program abuse and quality of care issues. In order to prove such cases, the PSC BI unit shall document a long-standing pattern of care where educational contacts have failed to change the abusive pattern. Isolated instances and statistical samples are not actionable. Medical doctors must be willing to testify.

Authority under §1156 of the Act is delegated to OIG to exclude practitioners and other persons who have been determined by a QIO to have violated their obligations under §1156 of the Act. To exclude, the violation of obligation under §1156 of the Act must be a substantial violation in a substantial number of cases or a gross and flagrant violation in one or more instances. Payment is not made for items and services furnished by an excluded practitioner or other person. Section 1156 of the Act also contains the authority to impose a monetary penalty in lieu of exclusion. Section 1156 exclusion actions and monetary penalties are submitted by QIOs to the OIG/OI.

Payment is not made for items and services furnished by an excluded practitioner or other person.

4.19.2.2 - Identification of Potential Exclusion Cases

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI unit shall review and evaluate abuse cases to determine if they warrant exclusion action. Examples of abuse cases suitable for exclusion include, but are not limited to:

- Providers who have been the subject of an adverse QIO finding.

- Providers whose claims must be reviewed continually because of repeated instances of overutilization.

- Providers who have been the subject of previous cases that were not accepted for prosecution because of the low dollar value, or who were the subject of previous cases that were settled without exclusion.

- Providers who furnish or cause to be furnished items or services that are substantially in excess of the patient's needs or are of a quality that does not meet professionally recognized standards of health care (whether or not eligible for benefits under Medicare, Medicaid, title V or title XX).

- Providers who are the subject of prepayment review for an extended period of time (longer than 6 months) who have not corrected their pattern of practice after receiving educational/warning letters.

- Providers who have been convicted of a program related offense (§1128(a) of the Social Security Act).

- Providers who have been convicted of a non-program related offense (e.g., a conviction related to neglect or abuse of a patient, or related to a controlled substance) (§1128(a) of the Social Security Act).

Also, §1833(a)(1)(D) of the Act provides that payment for clinical diagnostic laboratory tests is made on the basis of the lower of the fee schedule or the amount of charges billed for such tests. Laboratories are subject to exclusion from the Medicare program under §1128(b)(6)(A) of the Act where the charges made to Medicare are substantially in excess of their customary charges to other clients. This is true regardless of the fact that the fee schedule exceeds such customary charges.

Generally, to be considered for exclusion due to abuse, the practices have to consist of a clear pattern that the provider/supplier refuses or fails to remedy in spite of efforts on the part of the PSC, AC, *MAC*, or QIO groups. An exclusion recommendation is implemented only where efforts to get the provider/supplier to change the pattern of practice are unsuccessful. The educational or persuasive efforts are not necessary or desirable when the issues involve life-threatening or harmful care or practice.

If a case involves the furnishing of items or services in excess of the needs of the individual or of a quality that does not meet professionally recognized standards of health care, PSC BI units shall make every effort to obtain reports confirming the medical determination of their medical review from one or more of the following:

- The QIO for the area served by the provider/supplier
- State or local licensing or certification authorities
- QIO committees
- State or local professional societies
- Other sources deemed appropriate

4.19.2.3 - Development of Potential Exclusion Cases

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

A. Case Considerations

When PSC BI units recommend cases to OIG/OI for exclusion, they shall consider:

- The nature and seriousness of the acts in question
- Actions taken to persuade the provider/supplier to abstain from further questionable acts
- The experience gained from monitoring payments to the provider/supplier after corrective action was taken
- The degree of deterrence that might be brought about by exclusion
- The effects of exclusion on the delivery of health care services to the community
- Any other factors deemed appropriate

In cases recommended to OIG/OI for exclusion where there has **not** been a conviction, see 42 U.S.C. 1320 a-7(b).

Documentation for excessive services and charges shall include the length of time that the problem existed and the dollars lost by the program. Documentation of excessive services or poor quality of care requires a medical opinion from a qualified physician who must be willing to testify. All cases involving excessive services or poor quality of care shall also contain documentation of prior unsuccessful efforts to correct the problem through the use of less serious administrative remedies.

B. Notification to Provider

If, as a result of development of potential fraud or abuse, a situation is identified that meets one or more of the criteria in PIM Chapter 4, §4.19.2.1, PSC BI units shall consult the OIG/OI/OCIG (Office of Counsel to the Inspector General) contact person. The OIG prepares and sends a written notice to the provider containing the following information:

- Identification of the provider.
- The nature of the problem.
- The health care services involved.
- The basis or evidence for the determination that a violation has occurred. In cases concerning medical services, make every effort to include reports and opinions from a QIO or a QIO committee, or a state/local professional society.
- The sanction to be recommended.
- An invitation to discuss the problem with PSC BI unit and OIG/OI staff, or to submit written information regarding the problem.
- A statement that a recommendation for consideration of sanctions will be made to the OIG/OI within 30 days, if the problems are not satisfactorily resolved.

If the provider/supplier accepts the invitation to discuss the issues, PSC BI units shall make a report of the meeting for the record. This does not have to be a professionally transcribed report. Copies of the letter to the provider/supplier and the provider response, or the summary of the meeting, shall be in the file.

The PSC BI units shall refer cases that demonstrate a strong fraud potential to OIG/OI for investigation.

The PSC BI units notify OIG/OI of any cases that reach the level where a provider/supplier is notified of a problem in accordance with this section, even if the provider is convinced that there was a legitimate reason for the problem or that the problem has been corrected. PSC BI units do not refer these cases to OIG/OI unless requested to do so.

The PSC BI units document and refer cases involving harmful care as rapidly as possible. They handle OIG/OI requests for additional information as priority items.

C. Additional Information

Additional information that may be of value in supporting a proposal to exclude includes any adverse impact on beneficiaries, the amount of damages incurred by the programs, and potential program savings.

D. Mitigating Circumstances

Any significant factors that do not support a recommendation for exclusion or that tend to reduce the seriousness of the problem may be found in 42 CFR Part 1001 and are also considered. One of the primary factors is the impact of the sanction action on the availability of health care services in the community. PSC BI units shall bring mitigating circumstances to the attention of OIG/OI when forwarding their sanction recommendation.

4.19.2.4 - Contents of Sanction Recommendation

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall include in the sanction recommendation (to the extent appropriate) the following information:

- Identification of the subject, including the subject's name, address, date of birth, social security number, and a brief description of the subject's special field of medicine. If the subject is an institution or corporation, include a brief description of the type of services it provides and the names of its officers and directors.

- A brief description of how the violation was discovered.

- A description of the subject's fraudulent or abusive practices and the type of health service(s) involved.

- A case-by-case written evaluation of the care provided, prepared by the PSC's, AC's, or *MAC's* MR staff, which includes the patient's medical records. This evaluation shall cite what care was provided and why such care was unnecessary and/or of poor quality. (The reviewer may want to consult with someone from their RO OCSQ.) Medicare reimbursement rules shall not be the basis for a determination that the care was not medically necessary. The reviewer shall identify the specific date, place, circumstance, and any other relevant information. If possible, the reviewer should review the medical records of the care provided to the patient before and after the care being questioned.

NOTE: A minimum of 10 examples shall be submitted in support of a sanction recommendation under §1128(b)(6)(B). In addition, none of the services being used to support the sanction recommendations shall be over 2 years old.

- Documentation supporting the case referral, e.g., records reviewed, copies of any letters or reports of contact showing efforts to educate the provider, profiles of the

provider who is being recommended for sanction, and relevant information provided by other program administrative entities.

- Copies of written correspondence and written summaries of the meetings held with the provider regarding the violation.

- Copies of all notices to the party.

- Information on the amount billed and paid to the provider for the 2 years prior to the referral.

- Data on program monies on an assigned/non-assigned basis for the last 2 years, if available.

- Any additional information that may be of value in supporting the proposal to exclude or that would support the action in the event of a hearing.

NOTE: All documents and medical records should be legible.

4.19.2.6 - Denial of Payment to an Excluded Party

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSCs shall not recommend payments to the AC or *MAC*, and ACs and *MACs* shall not make payment on any excluded individual or entity for items or services furnished, ordered, or prescribed in any capacity on or after the effective date of exclusion, except in the following cases:

- For inpatient hospital services or post-hospital SNF care provided to an individual admitted to a hospital or SNF before the effective date of the exclusion, make payment, if appropriate, for up to 30 days after that date.

- For home health services provided under a plan established before the effective date of exclusion, make payment, if appropriate, for 30 days after the date on the notice.

- For emergency items and services furnished, ordered, or prescribed (other than an emergency item or service furnished, ordered, or prescribed in a hospital emergency room) payment may be made to an excluded provider on or after the effective date of exclusion.

4.19.2.6.1 - Denial of Payment to Employer of Excluded Physician

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

If an excluded physician is employed in a hospital setting and submits claims for which payment is prohibited, the AC or *MAC* Part B carrier surveillance process usually detects and investigates the situation.

However, in some instances an excluded physician may have a salary arrangement with a hospital or clinic, or work in group practice, and may not directly submit claims for payment. If this situation is detected, Part B ACs and *MACs*:

- Contact the hospital/clinic/group practice and inform them that they are reducing the amount of their payment by the amount of federal money involved in paying the excluded physician

- Develop and refer to the PSC BI unit as a CMP case.

Upon referral from the AC or *MAC*, the PSC BI unit shall finalize the case and refer it to the OIG.

4.19.2.6.2 - Denial of Payment to Beneficiaries and Others

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

If claims are submitted after the effective date of the exclusion by a beneficiary for items or services furnished, ordered, or prescribed by an excluded provider in any capacity,

ACs *and MACs* shall:

- Pay the first claim submitted by the beneficiary and immediately give notice of the exclusion.

- Not pay the beneficiary for items or services provided by an excluded party more than 15 days after the date of the notice to the beneficiary or after the effective date of the exclusion, whichever is later. The regulatory time frame is 15 days; however, CMS allows an additional 5 days for mailing.

If claims are submitted by a laboratory or DME *supplier* for any items or services ordered by a provider in any capacity excluded under §1156, or any items or services ordered or prescribed by a physician excluded under §1128, ACs *and MACs* shall handle the claims as above.

A. Notice to Beneficiaries

To ensure that the notice to the beneficiary indicates the proper reason for denial of payment, ACs *and MACs* shall include the following language in the notice:

"We have received your claim for services furnished or ordered by _____ on _____. Effective _____, _____was excluded from receiving payment for any items and services furnished in any capacity to Medicare beneficiaries. This notice is to advise you that no payment will be made for any items or services furnished by _____ if rendered more than 20 days from the date of this notice."

B. Notice to Others

The Medicare Patient and Program Protection Act of 1987 provides that payment is denied for any items or services ordered or prescribed by a provider excluded under §§1128 or 1156. It also provides that payment cannot be denied until the supplier of the items and services has been notified of the exclusion.

If claims are submitted by a laboratory or a DME company for any items or services ordered or prescribed by a provider excluded under §§1128 or 1156, ACs and *MACs* shall:

- Pay the first claim submitted by the supplier and immediately give notice of the exclusion.

- Do not pay the supplier for items or services ordered or prescribed by an excluded provider in any capacity if such items or services were ordered or prescribed more than 20 days after the date of notice to the supplier, or after the effective date of the exclusion, whichever is later.

To ensure that the notice to the supplier indicates the proper reason for denial of payment, ACs and *MACs* shall include the following language in the notice:

"We have received your claim for services ordered or prescribed by _____ on _____. Effective _____, _____was excluded from receiving payment for items or services ordered or prescribed in any capacity for Medicare beneficiaries. This notice is to advise you that no payment will be made for any items or services ordered or prescribed by _____ if ordered or prescribed more than 20 days from the date of this notice."

4.19.4 - Reinstatements

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

A provider may apply for reinstatement when the basis for exclusion has been removed, at the expiration of the sanction period, or any time thereafter. PSC BI units shall refer all requests they receive for reinstatement to the Office of Investigation of the OIG. Also, they furnish, as requested, information regarding the subject requesting reinstatement. OIG notifies the PSC BI unit in the state where the subject lives/practices of all reinstatements.

4.19.4.1 - Monthly Notification of Sanction Actions

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The Medicare Exclusion Database is a standard format, cumulative exclusion database that contains information on all exclusions and reinstatement actions in Medicare, Medicaid, and other federal health care programs. CMS receives this information from the Office of Inspector General monthly.

The PSCs, ACs, and *MACs* shall use the information contained in the MED and the GAO Debarment list to:

- Determine whether a physician/practitioner/provider or other health care supplier who seeks approval as a provider of services in the Medicare/Medicaid programs is eligible to receive payment

- Ensure that sanctioned providers are not being inappropriately paid

The dates reflected on the MED are the effective dates of the exclusion. Exclusion actions are effective 20 days from the date of the notice. Reinstatements or withdrawals are effective as of the date indicated.

The MED shows the names of a number of individuals and entities where the sanction period has expired. These names appear on the MED because the individual or entity has not been granted reinstatement. Therefore, the sanction remains in effect until such time as reinstatement is granted.

The PSCs, ACs, and *MACs* shall check their systems to determine whether any physician, practitioner, provider, or other health care worker or supplier is being paid for items or services provided subsequent to the date they were excluded from participation in the Medicare program. In the event a situation is identified where inappropriate payment is being made, they shall notify OIG and take appropriate action to correct the situation. Also, PSC BI units shall consider the instructions contained in the CMP section of the PIM (PIM Chapter 4, §4.20ff).

The PSCs shall work with ACs *and MACs* to document a process in the JOA to make the AC *and MAC* aware of any payments to an excluded provider.

The ACs and *MACs* shall ensure that no payments are made after the effective date of a sanction, except as provided for in regulations at 42 CFR 1001.1901(c) and 489.55.

The ACs and *MACs* shall check payment systems periodically to determine whether any individual or entity who has been excluded since January 1982 is submitting claims for which payment is prohibited. If any such claims are submitted by any individual in any capacity or any entity who has been sanctioned under §§1128, 1862(d), 1156, 1160(b) or 1866(b) of the Act, PSCs BI units shall forward them to OIG/OI.

Also, ACs and *MACs* shall refer to the RO all cases that involve habitual assignment violators. In cases where there is an occasional violation of assignment by a provider, they shall notify the provider in writing that continued violation could result in a penalty under the CMPL.

4.20.1.2 - Purpose

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The central purpose of the CMP process is to promote compliance with the program rules and regulations. To achieve this, CMS and its PSCs, ACs, and *MACs* shall enforce the regulatory standards and requirements.

The ACs and *MACs* shall educate the industry and the public regarding compliance. PSCs, ACs, and *MACs* shall have a statutory obligation to ensure compliance with regulations. Therefore, the efforts of ACs and *MACs* to achieve compliance shall be directed toward promoting a clear awareness and understanding of the program through education. When these efforts for achieving voluntary compliance have failed, formal enforcement action shall be referred to the appropriate agency.

4.20.1.4 - Administrative Actions

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSCs, ACs, and *MACs* shall ensure that the program rules and regulations are being appropriately followed. If violations are noted (either through internal reviews or through a complaint process), ACs and *MACs* shall take the appropriate steps to inform and educate the provider of the non-compliance and encourage future compliance.

If, after a period of time, there is no significant change by the provider (the non-compliance continues), then a final warning notice of plans to propose a corrective action (such as a CMP) shall be issued by the AC or *MAC*. This notice shall be sent by certified mail (return receipt required) to ensure its receipt by the provider. The notice shall indicate that previous notifications sent to the provider failed to correct the problem, and that this is a final warning. Additionally, it shall indicate that any further continuation of the non-compliance will result in the matter being forwarded to CMS or the OIG for administrative enforcement. While not specifically assessing a monetary penalty amount, the notice shall indicate that this is one type of sanction that may be applied.

4.20.3.1 - Referral Process to CMS

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Compliance is promoted through both administrative and formal legal actions. Administrative compliance action shall first be attempted by ACs and *MACs* through education and warning letters that request the provider to comply with Medicare's rules and regulations. If the provider fails to take corrective action and continues to remain non-compliant, the AC *and MAC* shall make a referral to the PSC who shall forward it to the Primary GTL, Associate GTL, and SME and the CMS CO Director of the Division of Benefit Integrity Management Operations (see PIM Chapter 4, §4.20.3.2).

It is important for ACs and *MACs* to promote program compliance in their respective jurisdictions. The ACs and *MACs* shall ensure that all materials presented to providers through education, published bulletins, or written communication are clear and concise and accurately represent the facts of compliance versus non-compliance. Providers shall also be allowed the opportunity to present additional facts that may represent mitigating circumstances. PSC BI units shall consider this information in an objective manner before proceeding with a CMP referral to CMS.

When a PSC BI unit elects to make a CMP referral to CMS, the initial referral package shall consist of a brief overview of the case; supportive documentation is not required at such time. The initial referral package shall consist of:

1. Identification of the provider, including the provider's name, address, date of birth, Social Security number, Medicare identification number(s), and medical specialty. If the provider is an entity, include the names of its applicable owners, officers, and directors.

2. Identification of the CMP authorities to be considered (use the authorities identified in PIM Chapter 4, §4.20.2.1).

3. Identification of any applicable Medicare manual provisions.

4. A brief description of how the violations identified above were discovered, and the volume of violations identified.

5. Total overpayments due the program or the beneficiary(ies), respectively.

6. A brief chronological listing of events depicting communication (oral and written) between the AC or *MAC* and the provider.

7. A brief chronological listing of bulletins addressing the non-compliant area (starting with the bulletin released immediately prior to the first incident of non-compliance by the provider).

8. Any additional information that may be of value to support the referral.

9. The name and phone number of contacts at the PSC BI unit.

Upon receipt of the above information, CMS staff will review the materials and conduct follow-up discussions with the PSC BI unit regarding the referral. Within 90 days of receipt of the referral, CMS will notify the PSC BI unit of its decision to accept or decline the referral.

If CMS declines the referral, the PSC shall communicate this to the AC or the *MAC* to continue in their efforts to educate and promote compliance by the provider. The PSC BI unit shall also consider other (less severe) administrative remedies, which, at a minimum, may include revocation of assignment privileges, establishing prepayment or postpayment medical reviews, and referral of situations to state licensing boards or medical/professional societies, where applicable. In all situations where inappropriate Medicare payments have been identified, ACs and *MACs* shall initiate the appropriate steps for recovery.

If CMS accepts the referral, the PSC BI unit shall provide any supportive documentation that may be requested, and be able to clarify any issues regarding the data in the case file or PSC, AC, and *MAC* processes.

4.20.3.2 - Referrals to OIG

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Upon discovery of any case that may implicate any of the OIG's delegated CMP authority, regardless of whether there is any other pending activity, or whether the fraud case was closed, the PSC BI unit shall contact the OIG/OI Field Office to discuss the potential case. If this contact results in a referral, the PSC BI unit shall follow the same referral format as described in PIM, chapter 4, §4.18.1.4. If a referral is not made or a referral is declined, the PSC BI unit shall consider other administrative remedies, which, at a minimum, may include revocation of assignment privileges, establishing prepayment or postpayment medical reviews, and referral of situations to sate licensing boards or medical/professional societies, where applicable. In all situations where appropriate Medicare payments have been identified, ACs and *MACs* shall initiate the appropriate steps for recovery.

The PSC BI unit shall send to the OIG all cases, as appropriate, where an excluded provider or individual has billed or caused to be billed to the Medicare or Medicaid program for the furnishing of items or services after exclusion. Such misconduct is sanctionable under §1128A(a)(C)(1) of the Social Security Act.

The PSC BI unit shall send to CMS DBIMO all cases where the PSC BI unit believes that misuse has occurred of the Medicare name, symbols, emblems, or other violations as described in §1140 of the Social Security Act and in 42 CFR 1003.102(b)(7). CMS will be responsible for referring these types of cases to OIG. All such cases shall be sent to the following CMS address:

Centers for Medicare & Medicaid Services
Division of Benefit Integrity Management Operations
Mail Stop C3-02-16
7500 Security Blvd
Baltimore, MD 21244

4.20.4 - CMS Generic Civil Monetary Penalties Case Contents

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The following information, if available, shall be included as part of the CMP case package and made available upon request by CMS:

1. Background information:

   a. All known identification numbers (PIN, UPIN, etc.).

   b. Provider's first and last name or entity name (if subject is an entity, also include the full name of the principal operator).

   c. Provider's address (street, city, state, and zip code). If violator is an entity, identify address where principal operator personally receives his/her mail.

2. Copies of any interviews, reports, or statements obtained regarding the violation.

3. Copies of documentation supporting a confirmation of the violation.

4. Copies of all applicable correspondence between beneficiary and provider.

5. Copies of all applicable correspondence (including telephone contacts) between the AC or *MAC* and provider.

6. Copies of provider's applicable bills to beneficiaries and/or ACs and *MACs*, and associated payment histories.

7. Copies of any complaints regarding provider and disposition of the complaint.

8. Copies of all publications (e.g., bulletins, newsletters) sent to provider by the PSC, AC, or *MAC* who discuss the type of violation being addressed in the CMP case.

9. Copies of any monitoring reports regarding the provider.

10. Name and telephone number of PSC BI unit contact.

4.20.5.1 - Beneficiary Right to Itemized Statement

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The following is background information for developing specific CMS CMP cases: Effective for services or items provided on or after January 1, 1999, §4311 of the Balanced Budget Act (BBA) provides that Medicare beneficiaries have the right to request and receive an itemized statement from their health care provider of service (e.g., hospital, nursing facility, home health agency, physician, non-physician practitioner, DMEPOS supplier). Upon receipt of this request, providers have 30 days to furnish the itemized statement to the beneficiary. Health care providers who fail to provide an itemized statement may be subject to a CMP of not more than $100 for each failure to furnish the information (§1806(b)(2)(B) of the Social Security Act). An itemized statement is defined as a listing of each service(s) or item(s) provided to the beneficiary. Statements that reflect a grouping of services or items (such as a revenue code) are not considered an itemized statement.

A beneficiary who files a complaint with an AC or *MAC* regarding a provider's failure to provide an itemized statement must initially validate that his/her request was in writing (if available), and that the statutory 30-day time limit (calendar days) for receiving the information has expired. In most cases, an additional 5 calendar days should be allowed for the provider to receive the beneficiary's written request. If the beneficiary did not make his/her request in writing, inform him/her that he/she must first initiate the request to the provider in writing. It is only after this condition and the time limit condition are met that the AC or *MAC* may contact the provider.

Once the AC or *MAC* confirms that the complaint is valid, the AC or *MAC* shall initiate steps to assist the beneficiary in getting the provider to furnish the itemized statement. ACs and *MACs* shall initiate the same or similar procedures when receiving complaints regarding mandatory submission of claims (i.e., communicating with the provider about their non-compliance and the possibility of the imposition of a CMP).

If the intervention of the AC or *MAC* results in the provider furnishing an itemized statement to the beneficiary, the conditions for the statute are considered met, and a CMP case should not be developed. Should the intervention of the AC or *MAC* prove unsuccessful, the AC or *MAC* shall consider referral to the PSC BI unit for subsequent referral of the potential CMP case to CMS, following the guidelines established in PIM Chapter 4, §§4.20.3.1 and 4.20.4. There may be instances where a beneficiary receives an itemized statement and the AC or *MAC* receives the beneficiary's request (written or oral) to review discrepancies on his/her itemized statement. ACs and *MACs* shall follow their normal operating procedures in handling these complaints. ACs and *MACs* shall determine whether itemized services or items were provided, or if any other irregularity (including duplicate billing) resulted in improper Medicare payments. If so, the AC or *MAC* shall recover the improper payments.

4.20.5.2 - Medicare Limiting Charge Violations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The Omnibus Budget Reconciliation Act of 1989 (OBRA) established a limitation on actual charges (balanced billing) by non-participating physicians. (Refer to §1848(g) of the Act, and Medicare Carriers Manual §§5000ff. and 7555, respectively, for further information.)

As a result of the reduction in limiting charge monitoring activities (i.e., the discontinuance of the Limiting Charge Exception Report and the Limiting Charge Monitoring Report, the discontinuance of sending compliance monitoring letters and Refund/Adjustment Verification Forms), developing a Limiting Charge CMP case shall require the following additional information:

- Contact with the provider - Based on CMS instructions, ACs and *MACs* are to assist beneficiaries in obtaining overcharge refunds from the providers. This assistance reinstates the activity of sending the refund verification forms and compliance monitoring letters respective to the beneficiary(ies) who request assistance. Copies of these communications will become part of the CMP case file. Ensure that the communication includes language that reminds the provider that the limiting charge amounts for most physician fee schedule services are listed on the disclosure reports they receive in their yearly participation enrollment packages. (This constitutes "notice" of the Medicare charge limits for those services.) The provider's letter should also include information that describes "what constitutes a violation of the charge limit," and that providers are provided notification on their copy of the remittance statements when they exceed the limiting charge. Providers who elected not to receive remittance statements for non-assigned claims should be reminded that they are still bound by the limiting charge rules, and that they are required to make refunds of overcharges. It may be appropriate at this time for providers to reconsider their decision not to receive remittance forms for non-assigned claims. Providers should also be informed of what action to take in order to receive these statements.

- Limiting Charge Monitoring Reports (LCMRs) - Produce LCMRs for all limiting charge violations respective to the provider and which encompasses the last three years. ACs and *MACs* shall also identify those beneficiaries appearing on the reports who have requested assistance in obtaining a refund from their provider.

4.21 - Monitor Compliance

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall follow-up on all incidences of documented false claims to ensure that the problem has not recurred and no longer exists. They shall send a letter to the provider indicating that they are monitoring their actions.

4.21.1 - Resumption of Payment to a Provider - Continued Surveillance After Detection of Fraud

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

After completion of the investigation and appropriate legal action, all determined overpayments are recouped by either direct refund or offset against payments being held in suspense. Once recoupment is completed, PSC BI units shall release any suspended monies that are not needed to recoup determined overpayments and, if applicable, penalties.

PSC BI units shall monitor future claims and related actions of the provider for at least 6 months, to assure the propriety of future payments. In addition to internal screening of the claims, if previous experience or future billings warrant, they shall periodically interview a sampling of the provider's patients to verify that billed services were actually furnished.

If, at the end of a 6-month period, there is no indication of a continuing aberrant pattern, PSC BI units shall discontinue the monitoring.

4.22 - Discounts, Rebates, and Other Reductions in Price

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

A PSC that learns of a questionable discount program shall contact OIG/OI to determine how to proceed. OIG/OI may ask for immediate referral of the matter for investigation.

4.22.1.1 - Marketing to Medicare Beneficiaries

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

This section explains marketing practices that could be in violation of the Medicare anti-kickback statute, 42 U.S.C. 1320a-7b(b). These practices shall comply with the Medicare anti-kickback statute and with the Office of the Inspector General's Compliance Program Guidance for the Durable Medical Equipment, Prosthetics, Orthotics and Supply Industry.

Marketing practices may influence Medicare beneficiaries who utilize medical supplies, such as blood glucose strips, on a repeated basis. Beneficiaries are advised to report any instances of fraudulent or abusive practices, such as misleading advertising and excessive or non-requested deliveries of test strips, to their *durable medical equipment medicare administrative contractors*.

Advertising incentives that indicate or imply a routine waiver of coinsurance or deductibles could be in violation of 42 U.S.C. 1320a-7b(b). Routine waivers of coinsurance or deductibles are unlawful because they could result in: 1) false claims, 2) violation of the anti-kickback statute, and/or 3) excessive utilization of items and services paid for by Medicare.

In addition, 42 U.S.C. 1320a-7a(a) (5) prohibits a person from offering or transferring remuneration. Remuneration is a waiver of coinsurance and deductible amounts, with exceptions for certain financial hardship waivers that are not prohibited.

Suppliers should seek legal counsel if they have any questions or concerns regarding waivers of deductibles and/or coinsurance or the propriety of marketing or advertising material.

Any supplier who routinely waives co-payments or deductibles can be criminally prosecuted and excluded from participating in federal health care programs.

4.22.2 - Cost-Based Payment (Intermediary *and Medicare Administrative Contractor* Processing of Part A Claims): Necessary Factors for Protected Discounts

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

For a discount to be protected, certain factors must exist. These factors assure that the benefit of the discount or rebate will be reported and passed on to the programs. If the buyer is a Part A provider, it must fully and accurately report the discount in its cost report. The buyer may note the submitted charge for the item or service on the cost report as a “net discount.” In addition, the discount must be based on purchases of goods or services bought within the same fiscal year. However, the buyer may claim the benefit of a discount in the fiscal year in which the discount is earned or in the following year. The buyer is obligated, upon request by DHHS or a state agency, to provide information given by the seller relating to the discount.

The following types of discounts may be protected if they comply with all the applicable standards in the discount safe harbor:

- Rebate check
- Credit or coupon directly redeemable from the seller
- Volume discount or rebate

The following types of discounts are not protected:

- Cash payment
- Furnishing one good or service free of charge or at a reduced charge in exchange for any agreement to buy a different good or service
- Reduction in price applicable to one payer but not to Medicare or a state health care program
- Routine reduction or waiver of any coinsurance or deductible amount owed by a program beneficiary

NOTE: There is a separate safe harbor for routine waiver of co-payments for inpatient hospital services.

4.22.3 - Charge-Based Payment (Intermediary *and Medicare Administrative Contractor* Processing of Part B Claims): Necessary Factors for Protected Discounts

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

For a discount program to be protected for Part B billing, certain factors shall exist. These factors assure that the benefit of the discount or other reduction in price is reported and passed on to the Medicare or Medicaid programs. A rebate rendered after the time of sale is not protected under any circumstances. The discount must be made at the time of sale of the good or service. In other words, rebates are not permitted for items or services if payable on the basis of charges. The discount must be offered for the same item or service that is being purchased or furnished. The discount must be clearly and accurately reported on the claim form.

Credit or coupon discounts directly redeemable from the seller may be protected if they comply with all the applicable standards in the discount safe harbor.

The following types of discounts are not protected:

- Rebates offered to beneficiaries

- Cash payment

- Furnishing an item or service free of charge or at a reduced charge in exchange for any agreement to buy a different item or service

- Reduction in price applicable to one payer but not to Medicare or a state health care program

- Routine reduction or waiver of any coinsurance or deductible amount owed by a program beneficiary

NOTE: There is a separate safe harbor for routine waiver of co-payments for inpatient hospital services.

4.23 - Hospital Incentives

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

As many hospitals have become more aggressive in their attempts to recruit and retain physicians and increase patient referrals, physician incentives (sometimes referred to as “practice enhancements”) are becoming increasingly common. Some physicians actively solicit such incentives. These incentives may result in reductions in the physician's professional expenses or an increase in their revenues. In exchange, the physician is aware that he or she is often expected to refer the majority, if not all, of his or her patients to the hospital providing the incentives.

The OIG has become aware of a variety of hospital incentive programs used to compensate physicians (directly or indirectly) for referring patients to the hospital. These arrangements are prohibited by the anti-kickback statute because they can constitute remuneration offered to induce, or in return for, the referral of business paid for by Medicare or Medicaid.

These incentive programs can interfere with the physician's judgment of what is the most appropriate care for a patient. They can inflate costs to the Medicare program by causing physicians to inappropriately overuse the services of a particular hospital. The incentives may result in the delivery of inappropriate care to Medicare beneficiaries and Medicaid recipients by inducing the physician to refer patients to the hospital providing financial incentives rather than to another hospital (or non-acute care facility) offering the best or most appropriate care for that patient. Indicators of potentially unlawful activity include:

- Payment of any sort by the hospital each time a physician refers a patient to the hospital.

- The use of free or significantly discounted office space or equipment (in facilities usually located close to the hospital).

- Provision of free or significantly discounted billing, nursing, or other staff services.

- Free training for a physician's office staff in areas such as management techniques, CPT coding, and laboratory techniques.

- Guarantees which provide that, if the physician's income fails to reach a predetermined level, the hospital supplements the remainder up to a certain amount.

- Low-interest or interest-free loans, or loans that may be “forgiven” if a physician refers patients (or some number of patients) to the hospital.

- Payment of the cost of a physician's travel and expenses for conferences.

- Payment for a physician's continuing education courses.

- Coverage on hospital's group health insurance plans at an inappropriately low cost to the physician.

- Payment for services (which may include consultations at the hospital) that require few, if any, substantive duties by the physician, or payment for services in excess of the fair market value of services furnished.

When PSC BI units learn of a questionable hospital incentive program, the matter shall be referred to OIG/OI.

The PSC BI units shall not provide, in writing or orally, an opinion on whether or not a particular business arrangement is in violation of the kickback law.

4.24 - Breaches of Assignment Agreement by Physician or Other Supplier

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

A. Criminal Penalty

The law provides that any person who accepts an assignment of benefits under Medicare, and who "knowingly, willfully, and repeatedly" violates the assignment agreement, shall be guilty of a misdemeanor and subject to a fine of not more than $2,000, or imprisonment of not more than 6 months, or both.

B. Administrative Sanction

The CMS may revoke the right of a physician (or other supplier, or the qualified reassignee of a physician or other supplier) to receive assigned benefits, if the physician (or other party) who has been notified of the impropriety of the practice:

- Collects or attempts to collect more than the Medicare-allowed charge as determined for covered services after accepting assignment of benefits for such items or services, or

- Fails to stop collection efforts already begun or to refund monies incorrectly collected.

C. Civil Monetary Penalties (CMPs)

The statute provides for CMPs of up to $2,000 per item or service claimed against any person who violates an assignment agreement.

D. Action by ACs *and MACs* on Receipt of Initial Complaint

Upon receipt of the initial assignment agreement violation complaint or complaints against a physician, ACs *and MACs* shall develop the facts to ascertain whether the allegation is valid, regardless of whether the complaint is referred from an SSA FO, an OIFO, a beneficiary, or the RO.

If a violation has occurred, the AC *and MAC* shall contact the physician in person, by phone, or by mail to explain the obligations assumed in accepting assignment and to obtain his/her assurance that improperly collected monies are being refunded and that further billings in violation of the assignment agreement will cease. The AC *and MAC* shall inform the physician of the possible criminal penalty discussed in subsection A (above), the possible administrative sanction (i.e., revocation of the assignment privilege) discussed in subsection B, and the possible CMPs discussed in subsection C. The dates and other particulars of the contact with the physician shall be recorded.

The AC *and MAC* shall supplement any personal or phone contact with a letter to the physician explaining his/her assignment obligations and the possible sanctions. The AC *and MAC* shall close the case with that letter if the physician response is satisfactory.

A satisfactory response shall include, at a minimum, the following:

- The physician acknowledges the obligations of the assignment agreement and agrees:
    - To make any necessary refund
    - To credit the refund due against other amounts owed, and
    - To stop further incorrect billing and to refund or credit any amount due the complainant as verified by the AC *and MAC*.

If the physician response is unsatisfactory, the AC *and MAC* shall refer the case to the PSC or the BI unit for further action. The action taken by the PSC BI unit depends on the circumstances. If the physician persists in billing the patient for the charges that gave rise to the complaint or fails to make any refund due, the PSC BI unit shall develop (including completion of the SSA-2808, if received) (see PIM chapter 4, §4.24H) and refer the case to the RO for initiation of steps to revoke the physician's assignment privilege. However, the RO may find it desirable to give the physician further written warning before undertaking such action.

If the physician, after having been warned, has violated his/her assignment agreement in connection with additional claims, see subsection E, below.

E. Action by Program Safeguard Contractor Benefit Integrity Unit When Violations Occur After Warning

Upon receipt of a new assignment violation complaint(s) after a physician has been given the warning described in subsection D, the PSC BI unit shall develop the facts and shall refer the case to the RO with a report, regardless of whether the complaint is referred from an SSA FO, OIFO, or RO. PSC BI units may wish to substitute an oral report to the RO in situations where the PSC BI unit has resolved the repeat violation. The RO considers whether to initiate action to revoke the physician's assignment privilege.

F. Procedure for Revoking Assignment Privilege

The RO may revoke assignment privileges when prosecution is inappropriate or not feasible. The RO notifies the physician of the proposed revocation of his right to receive assigned benefits and gives him/her 15 days to submit a statement, including any pertinent evidence, explaining why his/her right to payment should not be revoked. After the statement is received, or the 15-day period expires without the filing of the statement, the RO determines whether to revoke the physician's right to receive payment. If the determination is to revoke the physician's right to receive payment, the RO notifies the AC *and MAC* to suspend payment on all assigned claims received after the effective date of the revocation. The RO also notifies the physician of the revocation, and of his/her right to request a formal hearing on the revocation within 60 days. (The RO may extend the period for requesting a hearing.)

If the physician requests a formal hearing (to be conducted by a member of the Hearing Staff of the Office of Budget and Administration, CMS) and the hearing officer reverses the revocation determination, the RO instructs the AC *and MAC* to pay the physician's claims.

If the hearing officer upholds the revocation determination, or if no request for a hearing is filed during the period allowed, the RO instructs the AC *and MAC* to make any payments otherwise due the physician to the beneficiary who received the services or to another person or organization authorized under the law and regulations to receive the payments. (See the IOM, Claims Processing Manual, Pub. 100-04, chapter 1, §30.2 for payment to a representative payee or legal representative.) If the beneficiary is deceased, ACs *and MACs* shall make payment in accordance with the requirements of the IOM, Claims Processing Manual, Pub. 100-04, chapter 1, §§30.2.15, 50.1.3-50.1.6 to the person who paid the claim, to the legal representative of the beneficiary's estate, or to his/her survivors. (ACs *and MACs* shall not make payment to the physician.) The revocation remains in effect until the RO finds that the reason for the revocation has been removed and there is reasonable assurance that it will not recur. The RO's decision to continue the revocation is not appealable.

When the right of a person or organization to receive assigned payment is revoked, the revocation applies to any benefits payable to that person or organization throughout the country. The RO is responsible for notifying those ACs *and MACs* who are likely to receive claims.

See IOM, Pub. 100-04, chapter 1, §§30.2-30.2.8.3 for the effect of revocation of a physician's or other person's assignment privileges on the right of a hospital or other entity to accept assignment for his/her services. This section also contains information concerning the effect of revocation of a hospital's or other entity's assignment privileges on the right of a physician or other person for whom it has been billing to bill for his/her own services.

G. Other Considerations

Because of the government's responsibility to prosecute persons who repeatedly violate the assignment agreement, effective monitoring of such offenses is very important. The factors involved in each case may vary, and PSC BI units shall discuss with the RO, OIFO as appropriate, any situation where the PSC BI units believe that legal or administrative action is necessary. In addition, PSC BI units shall utilize the specific control measures and referral procedures in accordance with RO/OIG-OI direction. The RO may review the AC's *and MAC's* actions to assure that assignment violations are being properly tracked and reported.

The ACs *and MACs* shall notify physicians and other suppliers of the implications of §1842(b)(3)(ii) of the Act, since the penalties for violations of the assignment agreement are significant. ACs *and MACs* shall use the language contained in these letters, or similar language, when contacting providers regarding assignment violation. ACs *and MACs* shall ensure that all physicians are made aware of the penalties that can be imposed. This deters assignment violations and works against a defense by physicians that they had no knowledge of these laws.

H. Form for Reporting Assignment Agreement Violations

Form SSA-2808, Notice of Reported Assignment Agreement Violation, is specifically designed for SSA FOs and ACs *and MACs* to use in handling assignment agreement violations. SSA FOs use this form for referral and control of complaints. ACs *and MACs* use it to report action on complaints.

SSA FOs are responsible for completing sections one and two completely and clearly. They are to forward the original plus one copy and a second copy is to be sent to the servicing RO. A third copy is kept by the SSA FO for control and follow-up purposes. A fourth copy is sent to the appropriate RO for informational purposes.

In the event that there is an undue delay (in excess of 45 days) by the AC *and MAC* in processing complaints, the SSA FO sends periodic interim reports (monthly) to beneficiaries/complainants informing them that as soon as action is taken, notification will be sent to them. This action precludes excessive inquiries to the AC *and MAC*. If an SSA FO wishes to determine the status of the complaint, it contacts the RO.

The ACs *and MACs* shall complete section 3 of the Form SSA-2808 and forward a copy to the RO when appropriate action is completed. The RO notifies the originating SSA FO of the action taken.

4.25 - Participation Agreement and Limiting Charge Violations

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Section 2306 of the Deficit Reduction Act of 1984 established a physician/supplier participation program. The Omnibus Budget Reconciliation Act of l989 established a limitation on actual charges by non-participating physicians (see §1848(g) of the Act). Participating physicians/suppliers who violate their participation agreements, and non-participating physicians who knowingly, willfully, and repeatedly increase their charges to Medicare beneficiaries beyond the limits, are liable for action in the form of CMPs, assessments, and exclusion from the Medicare program for up to 5 years, or both. Criminal penalties also apply to serious violations of the participation agreement provisions.

For further discussion of the participation agreement and limiting charge provisions, see *IOM Pub.100-04, chapter 1, §§30.3 and 30.3.12.3.*

4.26 – Supplier Proof of Delivery Documentation Requirements

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Suppliers are required to maintain proof of delivery documentation in their files. Documentation must be maintained in the supplier's files for 7 years.

Proof of delivery is required in order to verify that the beneficiary received the DMEPOS. Proof of delivery is one of the supplier standards as noted in 42 CFR, 424.57(12). Proof of delivery documentation must be made available to the *DME MAC* upon request. For any services, which do not have proof of delivery from the supplier, such claimed items and services shall be denied and overpayments recovered. Suppliers who consistently do not provide documentation to support their services may be referred to the OIG for investigation and/or imposition of sanctions.

4.26.1 - Proof of Delivery and Delivery Methods

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

For the purpose of the delivery methods noted below, **designee** is defined as:

"Any person who can sign and accept the delivery of durable medical equipment on behalf of the beneficiary."

Suppliers, their employees, or anyone else having a financial interest in the delivery of the item are prohibited from signing and accepting an item on behalf of a beneficiary (i.e., acting as a designee on behalf of the beneficiary). The relationship of the designee to the beneficiary should be noted on the delivery slip obtained by the supplier (i.e., spouse, neighbor). The signature of the designee should be legible. If the signature of the designee is not legible, the supplier/shipping service should note the name of the designee on the delivery slip.

Suppliers may deliver directly to the beneficiary or the designee. An example of proof of delivery to a beneficiary is having a signed delivery slip, and it is recommended that the delivery slip include: 1) The patient's name; 2) The quantity delivered; 3) A detailed description of the item being delivered; 4) The brand name; and 5) The serial number. The date of signature on the delivery slip must be the date that the DMEPOS item was received by the beneficiary or designee. In instances where the supplies are delivered directly by the supplier, the date the beneficiary received the DMEPOS supply shall be the date of service on the claim.

If the supplier utilizes a shipping service or mail order, an example of proof of delivery would include the service's tracking slip, and the supplier's own shipping invoice. If possible, the supplier's records should also include the delivery service's package identification number for that package sent to the beneficiary. The shipping service's tracking slip should reference each individual package, the delivery address, the corresponding package identification number given by the shipping service, and if possible, the date delivered. If a supplier utilizes a shipping service or mail order, suppliers shall use the shipping date as the date of service on the claim.

Suppliers may also utilize a return postage-paid delivery invoice from the beneficiary or designee as a form of proof of delivery. The descriptive information concerning the DMEPOS item (i.e., the patient's name, the quantity, detailed description, brand name, and serial number) as well as the required signatures from either the beneficiary or the beneficiary's designee should be included on this invoice as well.

For DMEPOS products that are supplied as refills to the original order, suppliers must contact the beneficiary prior to dispensing the refill. This shall be done to ensure that the refilled item is necessary and to confirm any changes/modifications to the order. Contact with the beneficiary or designee regarding refills should take place no sooner than approximately 7 days prior to the delivery/shipping date. For subsequent deliveries of refills, the supplier should deliver the DMEPOS product no sooner than approximately 5 days prior to the end of usage for the current product. This is regardless of which delivery method is utilized. *DME MACs* shall allow for the processing of claims for refills delivered/shipped prior to the beneficiary exhausting his/her supply.

For those patients that are residents of a nursing facility, upon request from the *DME MAC*, suppliers should obtain copies of the necessary documentation from the nursing facility to document proof of delivery or usage by the beneficiary (e.g., nurse's notes).

4.27 - Annual Deceased-Beneficiary Postpayment Review

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

The PSC BI units shall identify and initiate actions to recover payments with a billed date of service that is after the beneficiary's date of death. The identification of improperly paid claims shall be performed at a minimum on an annual fiscal year basis for beneficiaries who died the previous fiscal year. In addition, the PSCs shall forward the identified overpayments to the AC *or MAC* for recoupment. The associated overpayment recoupment shall be initiated as soon as administratively possible.

EXAMPLE: Services rendered to beneficiaries who died during fiscal year 2002 - PSC BI units must identify improperly paid services. Upon identification, PSCs will refer this information to their respective AC or *MAC* for recoupment. ACs and *MACs* must issue associated overpayment demand letters as soon as administratively possible.

The PSCs, ACs, and *MACs* are not required to perform medical review for paid claims with dates of service after a beneficiary's date of death. PSC BI units shall identify the service that has been rendered after the beneficiary's date of death, and refer it to their respective AC or *MAC*. Subsequent notification to the provider that an improper payment has been made, for which recovery is being sought, shall be initiated by the AC or the *MAC*.

At a minimum, PSC BI units shall identify deceased beneficiaries and associated improperly paid claims by using one of the following two options:

- Utilize Internal Beneficiary Eligibility Records - This option involves performing a data extract against eligibility files for all beneficiaries within the PSC BI unit's jurisdiction and identifying those beneficiaries who have died during the applicable fiscal year. Once the list of deceased beneficiaries has been identified, PSC BI units utilize the claims processing history files to identify any services/claims containing a paid date of service that is after the CWF-posted date of death.

- Utilize External Beneficiary Eligibility Records - This option allows PSC BI units to utilize a CMS-created annual computer file of all deceased beneficiaries. On an annual calendar year basis, CMS creates computer files of all Medicare beneficiaries who died in the preceding 2 calendar years. These computer files should be available for PSC BI units to download from the Data Center by mid-February of each year. PSC BI units then review the format for this file to determine if any changes have been made from the previous fiscal year file. There have been known instances where a beneficiary's date of death is reported in both calendar year files. If such a situation is determined, the PSC BI unit shall use the latest calendar year file as the date of death. In accordance with the Health Insurance Portability and Accountability Act of 1996, a security firewall has been installed to protect the privacy rights of deceased beneficiaries. This firewall prevents unauthorized users from gaining access to the files of deceased beneficiaries. Due to the confidential information within these files, PSC BI units will not be able to access them

without their secured authorized identification code being included in the CMS-allowed-access list associated with the files.

To have access to these files, the PSC BI unit shall submit the name of the person(s) who will be accessing the files, their CMS mainframe user identification number, the PSC name and contractor number, the PSC Task Order number, and a telephone number. Only the person(s) identified will be allowed access to the files. Submit this information via e-mail to the CO Director of the Division of Benefit Integrity Management Operations.

The annual computer files are located on CMS's mainframe computer and may be found using the dataset naming convention "c@pig.#dbpc.deceased.benes.dodyyyy", where "yyyy" is equal to the calendar year in which the beneficiaries died. The format for this file is a text file and may also be found using "c@pig.#dbpc.deceased.benes.format". For example, computer file "c@pig.#dbpc.deceased.benes.dod2001" contains information on all Medicare beneficiaries who died during calendar year 2001. Computer file "c@pig.#dbpc.deceased.benes.dod.2002" contains information on all Medicare beneficiaries who died during calendar year 2002. Download both computer files and manipulate the data to determine those beneficiaries who died during fiscal year 2002 (October 1, 2001 - September 30, 2002). Then utilize the claims processing history files to identify any services/claims containing a paid date of service that is after the posted date of death.

The PSC BI units may consider conducting analyses to determine if healthcare providers continue to bill inappropriately after the results of this review have been completed (i.e., overpayments have been demanded and education regarding inappropriate billings have taken place). The PSC BI units may consider developing an investigation on providers whose pattern of billings remains noncompliant.

On an annual basis, PSC BI units shall submit a report on the accounting of the improper payments identified by the PSC BI unit and respective overpayments recouped by the AC and *MAC*. This report shall be due on December 5th of each year and sent to the Primary GTL. The report shall also be sent via e-mail to the CO Director of the Division of Benefit Integrity Management Operations.

4.28 - Joint Operating Agreement

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

A Joint Operating Agreement (JOA) is a document developed by the PSC and the AC *and the PSC and the MAC* that delineates the roles and responsibilities for each entity specific to a Task Order.

As it applies to the PSC's task order, the JOA shall, at a minimum:

- Include a description and documentation of process/workflows that illustrate how the PSC and AC *and the PSC and the MAC* intend to interact with one another to complete each of the tasks outlined in the Task Order on a daily basis.

- Establish responsibility for who shall request medical records/documentation(s) not submitted with the claim.

- Ensure that the AC *and MAC* communicates to the PSC any interaction with law enforcement on requests for cost report information.

- Establish responsibility for how medical documentation that has been submitted without being requested shall be stored and tracked.

- Establish responsibility for how medical documentation that has been submitted without being requested shall be provided to the PSC if documentation becomes necessary in the review process.

- Mitigate risk of duplicate medical documentation requests.

- Ensure that there is no duplication of effort by the PSC and the AC *and the PSC and the MAC* (e.g., the AC *and MAC* must not re-review PSC work).

- Identify the JOA participants

- Describe the roles and responsibilities of the PSC and the AC *and the PSC and the MAC*

- Clearly define dispute resolution processes

- Describe communication regarding CMS changes

- Include systems information

- Include training and education

- Include complaint screening and processing (including the immediate referral by the AC *and MAC* second-level screening staff of provider complaints and immediate advisements to the PSC)

- Include data analysis

- Include suspension of payment

- Include overpayments processing

- *Include data to evaluate PSC edit effectiveness via a monthly report from the AC and the MAC*

- Include excluded providers

- Include voluntary refunds
- Include incentive Reward Programs
- Include appeals
- Include provider enrollment
- Include system edits and audits
- Include requests for information
- Include FOIA and Privacy Act responsibilities
- Include interaction with law enforcement
- Include fraud investigations
- Include prepayment reviews
- Include postpayment reviews
- *Include coordination on LCDs (applicable only to JOAs between DME PSCs and DME MACs*
- Include Harkin Grantees
- Include OIG Hotline referrals
- Include Self-Disclosures
- Include consent settlements
- *Include coordination on Provider Outreach and Education*
- Include securing email information
- Include JOA workgroup meetings
- Contain other items identified by CMS, the PSC, and/or AC*, and/or MAC*

4.31 – Vulnerability Report

(Rev. 176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

Program vulnerabilities can be identified through a variety of sources such as the Chief Financial Officer's Audit, Fraud Alerts, the General Accounting Office, the Office of Inspector General (OIG), and PSC operations, as examples. PSC BI units shall submit any identified program vulnerabilities to RO and CO on a quarterly basis (i.e., 1/15, 4/15, 7/15, and 10/15). The identified vulnerabilities shall also include recommendations for resolving the vulnerability, any action taken to resolve the vulnerability, and shall describe the detection methodology.

The PSC BI unit shall send a copy of the identified vulnerabilities to the Primary GTL and Associate GTL. The PSC BI unit shall send a copy of the identified vulnerabilities to the following address: vulnerability@cms.hhs.gov

Medicare Program Integrity Manual
Exhibits

Table of Contents
(Rev.176, 11-24-06)

Exhibit 37 – *Office of Inspector General, Office of Investigations Data Use Agreement*

(Rev.176, Issued: 11-24-06, Effective: 12-26-06, Implementation: 12-26-06)

DUA #: _____

(to be completed by CMS Staff)

OFFICE OF INSPECTOR GENERAL, OFFICE OF INVESTIGATIONS DATA USE AGREEMENT

I, _____, representing the Office of Inspector General (OIG), Office of Investigations (OI), will observe the following in the use of the Centers for Medicare & Medicaid Services (CMS) files released to me:

A. Purpose: _____

B. The following CMS data file(s) is/are covered under this Agreement.

Description of Data/File	*Year(s)*	*System of Record (to be completed by CMS Staff)*

1. *The files will be used only for purposes authorized by the Inspector General Act of 1978 or other applicable law.*

2. *No information in the files released to the OIG will be used or disclosed except in strict accordance with all applicable confidentiality laws and regulations. Where practicable and consistent with OIG oversight responsibilities, the OIG will notify CMS of files extracted or derived from these files are disclosed pursuant to Federal disclosure and confidentiality laws.*

3. *The information sought in this request is required to be produced to the Office of Investigations pursuant to the Inspector General Act 1978, U.S.C. App. The information is also sought by the OIG in its capacity as a health oversight agency, and this information is necessary to further health oversight activities. Disclosure is therefore permitted under the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. 164.501; 164.512(a); and 164.512(d).*

4. _____ *will be designated as custodian of these files and will be responsible for establishment and maintenance of security arrangements to prevent unauthorized use. If the custodianship is transferred within the organization, CMS will be notified.*

5. *No listings or information from individual records, with identifiers will be published or otherwise released outside of those deemed appropriate by OIG to perform the legal scope of OIG duties and responsibilities.*

6. *The OIG needs to retain these files for up to 10 years. CMS will contact the OIG representative at the end of 5 years to confirm either that data will be destroyed or that OIG has a continuing need for the data. CMS will document its tracking system to indicate OIG's need for retention or destruction.*

OIG Representative- Printed:	*Phone Number:*	*Email Address:*	
Street Address:	*City:*	*State:*	*Zip Code:*
Signature:	*Date:*		

Name of Custodian of Files, If Different:	*Phone Number:*	*E-mail Address:*	
Street Address:	*City:*	*State:*	*Zip Code:*
CMS Representative- Printed:			
Signature:	*Date:*		