CMS Manual System

Pub. 100-08 Medicare Program Integrity

Department of Health & Human Services (DHHS)
Centers for Medicare & Medicaid Services (CMS)

Transmittal 101 **Date: JANUARY 28, 2005**

CHANGE REQUEST 3579

SUBJECT: Benefit Integrity (BI) PIM Revisions

I. SUMMARY OF CHANGES: Various BI sections of the PIM were clarified or revised, and all references to Medicare Fraud Information Specialists (MFIS) were deleted.

NEW/REVISED MATERIAL - EFFECTIVE DATE*: February 28, 2005
IMPLEMENTATION DATE: February 28, 2005

Disclaimer for manual changes only: The revision date and transmittal number apply to the red italicized material only. 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:
(R = REVISED, N = NEW, D = DELETED)

R/N/D	CHAPTER/SECTION/SUBSECTION/TITLE
R	2/2.3/Sources of Data for PSCs
R	4/Table of Contents
R	4/4.2.2.4/Procedural Requirements
R	4/4.2.2.5/Reserved for Future Use
R	4/4.2.2.5.1/Reserved for Future Use
R	4/4.2.2.5.2/ Reserved for Future Use
R	4/4.2.2.6/Benefit Integrity Security Requirements
R	4/4.4.1/Requests for Information From Outside Organizations
R	4/4.4.2/Program Safeguard Contractor and Medicare Contractor Coordination With Other Program Safeguard Contractors and Medicare Contractors
R	4/4.6.2/Complaint Screening
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	4/4.11.1/Background
R	4/4/11.1.1/Information Not Captured in the FID
R	4/4/11.2.1/Initial Entry Requirements for Investigations

R	4/4.11.3.3/Designated PSC and Medicare Contractor BI Unit Staff and the Fraud Investigation Database
R	4/4.16/AC and PSC Coordination on Voluntary Refunds
R	4/4.17/Reserved for Future Use
R	4/4.18.1/Referral of Cases to the Office of the Inspector General/Office of Investigations
R	4/4.18.2/Referral to State Agencies or Other Organizations
R	4/4.20.2.2/Civil Monetary Penalties Delegated to OIG
R	4/4.27/Annual Deceased-Beneficiary Postpayment Review
R	4/4.31/Vulnerability Report

III. FUNDING: Medicare contractors shall implement these instructions within their current operating budgets.

IV. ATTACHMENTS:

X	**Business Requirements**
X	**Manual Instruction**
	Confidential Requirements
	One-Time Notification
	Recurring Update Notification

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

Attachment - Business Requirements

Pub. 100-08	Transmittal: 101	Date: January 28, 2005	Change Request 3579

SUBJECT: Benefit Integrity (BI) PIM Revisions

I. GENERAL INFORMATION

A. Background: One section in chapter 2 and various sections in chapter 4, of the PIM, were revised for clarification.

B. Policy: N/A

C. Provider Education: None.

II. BUSINESS REQUIREMENTS

"Shall" denotes a mandatory requirement
"Should" denotes an optional requirement

Requirement Number	Requirements	Responsibility ("X" indicates the columns that apply)									
		FI	PSC	RHHI	Carrier	DMERC	Shared System Maintainers				Other
							FISS	MCS	VMS	CWF	
3579.1	At a minimum, the denial data shall include data for edits that were requested and/or recommended by the PSC.	X	X	X	X	X					
3579.2	PSCs and Medicare contractor BI units shall follow the functions added in section 4.2.2.4 which were previously designated as MFIS functions. PSCs and Medicare contractor BI units are not required to have an MFIS, but they must perform the functions that were previously assigned to an MFIS.		X			X					
3579.3	References to MFIS (Medicare Fraud Information Specialist) in section 4.2.2.6 were deleted.					X					

Requirement Number	Requirements	Responsibility ("X" indicates the columns that apply)									
		FI	PSC	RHHI	Carrier	DMERC	Shared System Maintainers				Other
							FISS	MCS	VMS	CWF	
3579.4	Subsequent law enforcement requests for the same provider that are within the scope of the initial request do not have to be in writing.		X			X					
3579.5	References to MFIS were deleted in section 4.4.2.					X					
3579.6	The same complaint shall only be counted once in the same month. However, it is possible that the same complaint will be counted more than once from month to month (e.g., counted as opened in October; pending in November; and closed in December). Open indicates any complaints opened and pending in the reporting month.	X		X	X	X					
3579.7	If medical records are not received within 45 calendar days, the claim(s) shall be denied. However, if fraud is suspected when medical records are not received, these situations shall be referred to the PSC or Medicare contractor BI unit.	X	X	X	X	X					
3579.8	References to MFIS were deleted in section 4.10.1.					X					
3579.9	References to MFIS were deleted from section 4.10.2.					X					
3579.10	References to MFIS were deleted from section 4.10.3.					X					
3579.11	References to MFIS were deleted from section 4.10.4.					X					

Requirement Number	Requirements	Responsibility ("X" indicates the columns that apply)									
		FI	PSC	RHHI	Carrier	DMERC	Shared System Maintainers				Other
							FISS	MCS	VMS	CWF	
3579.12	References to MFIS were deleted from section 4.10.5.					X					
3579.13	Upon receipt of Waiver Alerts, PSCs and Medicare contractor BI units shall provide the Waiver information to their respective ACs or Medicare contractor unit to ensure that Medicare payments are not denied inappropriately.	X	X	X	X	X					
3579.14	References to MFIS were deleted from section 4.11.1.					X					
3579.15	References to MFIS were deleted from section 1.11.3.3.					X					
3579.16	PSCs and Medicare contractor BI units shall also monitor the MED for consistency.		X			X					
3579.17	PSCs and Medicare contractor BI units shall send one letter annually to the same provider submitting a voluntary refund, advising the provider of the following: During the past year, you have submitted refunds to your Medicare carrier or fiscal intermediary. Please be advised that this repayment of funds 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 those claims.		X			X					
3579.18	The requirement in section 4.18.1 to consult law enforcement within 60 days of identifying the need for administrative action has been removed.		X			X					

Requirement Number	Requirements	Responsibility ("X" indicates the columns that apply)									
		FI	PSC	RHHI	Carrier	DMERC	Shared System Maintainers				Other
							FISS	MCS	VMS	CWF	
3579.19	PSCs and Medicare contractor 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.		X			X					
3579.20	References to MFIS were deleted from section 4.18.2.					X					
3579.21	Section 4.20.2.2 was revised to add a new authority, section 1860D-31(i)(3).		X			X					
3579.22	With regard to annual deceased beneficiary postpayment review, PSCs and Medicare contractor 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 PSCs and Medicare contractor BI units may consider developing an investigation on providers whose pattern of billings remains noncompliant.		X			X					
3579.23	PSCs and Medicare contractor BI units shall submit any identified program vulnerabilities to CMS RO and CO on a quarterly basis (i.e., 1/15, 4/15, 7/15, and 10/15).		X			X					
3579.24	The PSC and Medicare contractor BI unit shall also send the CMS CO a copy of the identified vulnerabilities to the following address: vulnerabilities@cms.hhs.gov.		X			X					

III. SUPPORTING INFORMATION AND POSSIBLE DESIGN CONSIDERATIONS

A. Other Instructions: N/A

X-Ref Requirement #	Instructions

B. Design Considerations: N/A

X-Ref Requirement #	Recommendation for Medicare System Requirements

C. Interfaces: N/A

D. Contractor Financial Reporting /Workload Impact: N/A

E. Dependencies: N/A

F. Testing Considerations: N/A

IV. SCHEDULE, CONTACTS, AND FUNDING

Effective Date*: February 28, 2005 **Implementation Date:** February 28, 2005 **Pre-Implementation Contact(s):** Kimberly Downin, kdownin@cms.hhs.gov **Post-Implementation Contact(s):** Kimberly Downin, kdownin@cms.hhs.gov	**Medicare contractors shall implement these instructions within their current operating budgets.**

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

2.3 – Sources of Data for PSCs

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

Medicare contractor BI units must follow PIM, chapter 2, §2.2. The following instructions in this section apply to PSCs only.

The PSCs' approach for combining claims data (fiscal intermediary, regional home health intermediary, carrier, and durable medical equipment regional carrier data) and other data to create a platform for conducting complex data analysis shall be documented in their Information Technology Systems Plan. By combining data from various sources, the PSC will present an entire picture of a beneficiary's claim history regardless of where the claim was processed. The primary source of this data will be the CMS National Claims History (NCH). The PSC shall be responsible for obtaining data for all beneficiaries for whom the AC(s) paid the claims.

PSCs are required to store at a minimum the most recent 36 months worth of data (including Part A, Part B, and DMERC) for the jurisdiction defined in their task order.

If the jurisdiction of the AC(s) is not defined geographically, the PSC shall obtain a complete beneficiary claims history for each unique beneficiary for whom the AC(s) paid a claim.

Example #1: The AC(s) jurisdiction being competed covers Maryland but includes a hospital chain with facilities in Montana. The PSC would request claims history from NCH for all claims paid by the AC(s).

Example #2: The AC(s) jurisdiction being competed covers Maryland, a beneficiary lives in Pennsylvania, and the beneficiary saw a doctor in Maryland. The PSC would request claims history from NCH for all claims paid by the AC(s).

PSCs will not be able to tap data from the Common Working File (CWF). The CMS Office of Information Services (OIS) has advised that this methodology for obtaining data will not be allowed.

PSCs may, if agreement and cooperation of the AC(s) are obtained, use data directly from the claims processing system of the AC(s), and then supplement the other data using NCH.

In developing this plan the PSCs shall address the above requirements and, at a minimum, establish read-only access to the AC's shared claims processing system(s) and access to the Part A, B, and D data available through the NCH for the jurisdictional area defined in the Task Order. The PSC shall also work with the AC(s) to obtain denial data and document the process for obtaining this data from the AC(s) in the Joint Operating Agreement. *At a minimum, the denial data shall include data for edits that were requested and/or recommended by the PSC.*

The PSC must have the ability to receive, load, and manipulate CMS data. The data must also be maintained in accordance with CMS and Federal privacy laws and regulations as described in the CMS Data Use Agreement. For planning purposes, the PSCs should assume that there are 30 claims per HIC per year, on average. A claim record is about 1000 bytes. To calculate the storage space necessary, use the following formula:

#HICs X 30 claims X #years X 1000 = #bytes

The CMS Government Task Leaders (GTL) and PSC will need to complete:

- Data Use Agreement to give permission to receive privacy protected data.
- Data Request form to specify all data required by the PSC.
- HDC Application for HDC access and/or CMS systems' access to get access to the data center and/or to specify which CMS systems the PSC will access.
- DESY system application form. (This is provided to the PSC post-award.)

Information on data files, including file layouts and data dictionaries, is available at http://cms.hhs.gov/data/purchase/default.asp.

Medicare Program Integrity Manual
Chapter 4 - Benefit Integrity

Table of Contents
(Rev. 101, 01-28-05)

4.2.2.4 - Procedural Requirements

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

Medicare contractors shall provide written procedures for Medicare contractor BI unit personnel and for personnel in other Medicare contractor components (claims processing, MR, beneficiary services, intermediary audit, etc.) to help identify potential fraud situations. Include provisions to ensure that personnel shall:

- Refer potential fraud cases promptly to the BI unit.
- Forward complaints alleging fraud through the second level screening staff to the BI unit.
- Maintain confidentiality of referrals to the BI unit so that the civil rights of those involved are protected.
- Forward to the BI unit documentation of the details of telephone or personal contacts involving fraud issues discussed with providers or provider staff, and retain such information in individual provider files.

In addition, PSCs and Medicare contractor BI units shall ensure the performance of the functions below and have written procedures for these functions:

- Keep educational/warning correspondence with providers and other fraud documentation concerning specific issues in individual provider files (refer to §4.2.2.4.2 for retention of this documentation), so that PSCs and Medicare contractors are able to retrieve such documentation easily.
- Maintain communication and information flowing between the PSC or Medicare contractor BI unit, and the PSC, AC, or Medicare contractor MR staff, and as appropriate, intermediary audit staffs.
- *Obtain and share information on health care fraud issues/fraud investigations among carriers (including durable medical equipment regional carriers (DMERCs)), fiscal intermediaries (including rural home health intermediaries (RHHIs)), PSCs, CMS, and law enforcement.*
- *Serve as a reference point for law enforcement and other organizations and agencies to contact when they need help or information on Medicare fraud issues and do not know whom to contact.*
- *Coordinate and attend fraud-related meetings/conferences and inform all appropriate parties about these meetings/conferences. These*

meetings/conferences include, but are not limited to, health care task force meetings and conference calls.

- *Distribute fraud alerts to the appropriate parties. Share PSC and Medicare contractor BI unit findings on fraud alerts with PSCs and Medicare contractors within the appropriate jurisdiction and CMS.*

- *Work with the GTL, Co-GTL, and SME (if a PSC) and CMS RO (if a Medicare contractor) to develop and organize external programs and perform training as appropriate for law enforcement, ombudsmen, grantees (e.g., Harkin Grantees) and other CMS health care partners (e.g., AoA, state MFCU).*

- *Serve as a resource to CMS as necessary. For example, serve as a resource to CMS on the FID, including FID training.*

- *Help to develop fraud-related outreach materials (e.g., pamphlets, brochures, videos) in cooperation with beneficiary services and/or provider relations departments of the ACs and Medicare contractors, for use in their training. Submit written outreach material to the CMS RO (if a Medicare contractor) and the GTL, Co-GTL, and SME (if a PSC) for clearance.*

- *Assist in preparation and development of fraud-related articles for AC and Medicare contractor newsletters/bulletins. The PSC and Medicare contractor BI unit shall send CMS CO a copy of these newsletters/bulletins to the following address:*

  Centers for Medicare & Medicaid Services (CMS)
  Re: Newsletter/Bulletin Articles
  Division of Benefit Integrity and Law Enforcement Liaison
  Mail Stop C3-02-16
  7500 Security Boulevard
  Baltimore, Maryland 21244

- *Provide resources and training for the development of internal and new hire fraud training.*

- Take appropriate administrative action on cases not accepted by OIG or other investigative agencies. At a minimum, provide information for recovery of identified overpayments and other corrective actions discussed in PIM, chapter 3, §8ff and §9ff.

- Properly prepare and document cases referred to OIG/OI; two copies of a summary page shall be included with each fraud referral made to the OIG. The referral format listed in PIM Exhibits 16.1 and 16.2 shall be followed, unless written guidance is provided by the applicable OIG/OI office and approved by the GTL, Co-GTL, and SME (if a PSC) or the applicable CMS RO (if a Medicare

contractor BI unit). PSCs and Medicare contractor BI units shall maintain files on the written guidance provided by the OIG/OI.

- Meet (in-person or telephone call) quarterly, or more frequently if necessary, with OIG agents to discuss pending or potential cases.

- Meet (in-person or telephone) regularly with DOJ to enhance coordination with them on current or pending cases.

- Furnish all available information upon request to OIG/OI with respect to excluded providers requesting reinstatement.

- Ensure that all cases that have been identified where a provider consistently fails to comply with the provisions of the assignment agreement are reported by the PSC to the GTL, Co-GTL, and SME; and reported by the Medicare contractor BI unit to the RO.

- Maintain documentation on the number of investigations alleging fraud, the number of cases referred to OIG/OI (and the disposition of those cases), processing time of investigations, and types of violations referred to OIG (e.g., item or service not received, unbundling, waiver of co-payment).

- Conduct investigations (including procedures for reviewing questionable billing codes), make beneficiary contacts (see PIM, chapter 4, §4.7.1 for details concerning investigations), and refer cases to and from the MR unit within your organization.

- Ensure that before making an unannounced visit where fraud is suspected, *obtain approval from* the GTL (if a PSC) or RO (if a Medicare contractor BI unit), and the OI Field Office, and ensure that any other appropriate investigative agency is also apprised of the plan. PSC and Medicare contractor BI unit staff shall never engage in covert operations (e.g., undercover or surveillance activities). *If OIG does not give approval, discuss this with the GTL (if a PSC) or RO (if a Medicare contractor) and they will make the final decision.*

- *Obtain approval* by email, letter, or telephone call*, and express any concerns* (if a telephone call, follow up with a letter or email) to the GTL (if a PSC) or to the RO (if a Medicare contractor BI unit) when the PSC or Medicare contractor BI unit is asked to accompany the OI or any other law enforcement agency when they are going onsite to a provider for the purpose of gathering evidence in a fraud case (e.g., executing a search warrant). However, law enforcement must make clear the role of PSC or Medicare contractor BI unit personnel in the proposed onsite visit. The potential harm to the case and the safety of PSC or Medicare contractor BI unit personnel shall be thoroughly evaluated. PSC or Medicare contractor BI unit personnel shall properly identify themselves as PSC or Medicare contractor BI unit employees, and under no circumstances shall they

represent themselves as law enforcement personnel or special agents. Lastly, under no circumstances shall PSC or Medicare contractor BI unit personnel accompany law enforcement in situations where their personal safety is in question.

ACs ensure the performance of the functions below and have written procedures for these functions:

- Ensure no payments are made for items or services ordered, referred, or furnished by an individual or entity following the effective date of exclusion (see PIM, chapter 4, §4.19ff for exceptions).

- Ensure all instances where an excluded individual or entity that submits claims for which payment may not be made after the effective date of the exclusion are reported to the OIG (see PIM, chapter 4, §4.19ff).

- Ensure no payments are made for an excluded individual or entity who is employed by a Medicare provider or supplier.

4.2.2.5 – *Reserved for Future Use*

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

4.2.2.5.1 – *Reserved for Future Use*

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

4.2.2.5.2 – *Reserved for Future Use*

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

4.2.2.6 – Benefit Integrity Security Requirements

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)
PSCs and Medicare contractors shall ensure a high level of security for this sensitive function. PSCs and Medicare contractor BI unit staff, as well as all other PSC and Medicare contractor employees, shall be adequately informed and trained so that information obtained by, and stored in, the PSC and Medicare contractor BI unit is kept confidential.

Physical and operational security within the PSC and Medicare contractor BI unit is essential. Operational security weaknesses in the day-to-day activities of PSCs and Medicare contractor BI units may be less obvious and more difficult to identify and correct than physical security. The interaction of PSCs and Medicare contractor BI units with other PSC or Medicare contractor operations, such as the mailroom, could pose potential security problems. Guidelines that shall be followed are discussed below.

Most of the following information can be found in the Business Partners Security Manual, which is located at http://www.cms.hhs.gov/manuals/117_systems_security. It is being reemphasized in this PIM section.

A - Program Safeguard Contractor and Medicare Contractor Benefit Integrity Unit Operations

PSC and Medicare contractor BI unit activities shall be conducted in areas not accessible to the general public and other non-BI Medicare contractor staff. Other requirements shall include:

- Complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provisions.

- Limiting access to PSC and Medicare contractor BI unit sites to only those who need to be there on official business. (Tours of the Medicare contractor shall not include the BI unit.)

- Ensuring that discussions of highly privileged and confidential information cannot be overheard by surrounding units. Ideally, the unit does not have an unmonitored entrance or exit to the outside, and has a private office for the manager, for the discussion of sensitive information.

- Ensuring that visitors to the PSC or Medicare contractor BI unit who are there for official purposes unrelated to PSC or Medicare contractor BI unit functions (e.g., cleaning crews, mail delivery personnel, technical equipment repair staff) are not left unobserved.

- Securing the PSC or Medicare contractor BI unit site when it is not occupied by PSC or Medicare contractor BI unit personnel.

- Barring budget constraints and a specific written waiver (exception) from the CMS RO, the Medicare contractor BI unit shall be completely segregated from all other Medicare contractor operations. This segregation shall include closed walls or partitions that prevent unauthorized access or overhearing of sensitive investigative information. 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.

B - Handling and Physical Security of Sensitive Material

PSCs and Medicare contractor BI units shall consider all fraud and abuse allegations and associated investigation and case material to be sensitive material. The term "sensitive material" includes, but is not limited to, PSC or Medicare contractor BI unit investigation and case files and related work papers (correspondence, telephone reports, complaints and associated records, personnel files, reports/updates from law enforcement, etc.). Improper disclosure of sensitive material could compromise an investigation or prosecution of a case; it could also cause harm to innocent parties or potentially jeopardize the personal safety of law enforcement (e.g., covert/undercover investigations).

The following guidelines shall be followed:

- 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 staff from the PSC, AC or Medicare contractor MR or audit units, data analysis, senior management, or corporate counsel.

- Ensure the mailroom, general correspondence, and telephone inquiries procedures maintain confidentiality whenever correspondence, telephone calls, or other communications alleging fraud are received. All internal written operating procedures shall clearly state security procedures.

- Mailroom staff shall be directed not to open BI unit mail in the mailroom, unless the mailroom staff has been directed to do so for safety and health precautions; mail contents shall not be read and shall be held in confidence. Mail being sent to CO, another PSC, or Medicare contractor BI unit shall be marked "personal and confidential," and shall be addressed to a specific person.

- Where not prohibited by more specialized instructions, sensitive materials may be retained at employees' desks, in office work baskets, and at other points in the office during the course of the normal work day. Access to these sensitive materials is restricted, and such material shall never be left unattended.

- For mail processing sites located in separate PSC or Medicare contractor facilities, the PSC or Medicare contractor shall minimize the handling of BI unit mail by multiple parties before delivery to the PSC or Medicare contractor BI unit.

- When not being used or worked on, such materials shall be retained in locked official repositories such as desk drawers, filing cabinets, or safes. Such repositories shall be locked at the end of the work day and at other times when immediate access to their contents is not necessary.

- Where such materials are not returned to their official repositories by the end of the normal work day, they shall be placed in some other locked repository (e.g., an employee's desk), locked office, or locked conference room.

- PSCs and Medicare contractor BI units shall establish procedures for safeguarding keys, combinations, codes and other mechanisms, devices, or methods for achieving access to the work site and to lockable official repositories. The PSCs and Medicare contractor BI units shall limit access to keys, combinations, etc., and maintain a sign-off log to show the date and time when repositories other than personal desk drawers and file cabinets are opened and closed, the documents accessed, and the name of the person accessing the material.

- The PSC and Medicare contractor BI unit shall maintain a controlled filing system (see PIM Chapter 4, §4.2.2.4.1).

- Discarded sensitive information shall be shredded on a daily basis or stored in a locked container for subsequent shredding.

C - Designation of a Security Officer

The PSC or Medicare contractor BI unit manager shall designate an employee to serve as the security officer of the PSC or Medicare contractor BI unit. In addition to their BI duties, the security officer's responsibilities shall include:

- Continuous monitoring of component operations to determine whether the basic security standards noted in B above are being observed.

- Correcting violations of security standards immediately and personally, where practicable and within his/her authority. (This refers to locking doors mistakenly left open; switching off computer equipment left on after the employee using it has departed for the day; locking file cabinets, desk drawers, storage (file) rooms, or safes left unlocked in error; and similar incidents where prompt action is called for.).

- Reporting violations of security standards to the appropriate supervisory authority, so that corrective and/or preventive action can be taken.

- Maintaining a log of all reviews and indicating any violations. The log shall identify the reported issue, the date reported, whom the issue was reported to, and any subsequent resolution. CMS staff may request to review this log periodically.

The PSC or Medicare contractor BI unit manager, compliance manager, or other designated manager shall:

- Review their general office security procedures and performance with the security officer at least once every 6 months.

- Document the results of the review.

- Take such action as is necessary to correct breaches of the security standards and to prevent recurrence. The action taken shall be documented and maintained by the PSC or Medicare contractor BI unit manager.

D - Staffing of the Program Safeguard Contractor or Medicare Contractor Benefit Integrity Unit and Security Training

The PSC or Medicare contractor BI unit manager shall ensure that PSC or Medicare contractor BI unit employees are well-suited to work in this area and that they receive appropriate CMS-required training.

All PSC or Medicare contractor BI unit employees should have easily verifiable character references and a record of stable employment.

The PSC or Medicare contractor BI unit manager shall ensure the following:

- Thorough background and character reference checks, including at a minimum credit checks, shall be performed for potential employees, to verify their suitability for employment with the PSC or Medicare contractor BI unit.

- In addition to a thorough background investigation, potential employees shall be asked whether their employment in the PSC or Medicare contractor BI unit might involve a conflict of interest.

- At the point a hiring decision is made for a PSC or Medicare contractor BI unit position, and prior to the person starting work, the proposed candidate shall be required to fill out a conflict of interest declaration as well as a confidentiality statement.

- Existing employees shall be required annually to fill out a conflict of interest declaration as well as a confidentiality statement.

- Temporary employees, such as those from temporary agencies, and students (non-paid or interns) shall not be employed in the PSC or Medicare contractor BI unit.

- The special security considerations under which the PSC or Medicare contractor BI unit operates shall be thoroughly explained and discussed.

- The hiring of fully competent and competitive staff, and the implementation of measures to foster their retention.

E - Access to Information

PSC, Medicare contractor, and CMS managers shall have routine access to sensitive information if the PSCs, Medicare contractors, and CMS managers are specifically authorized to work directly on a particular fraud case or are reviewing cases as part of their oversight responsibilities and their performance evaluations. This includes physician consultants who may be assisting the BI unit and whose work may benefit by having specific knowledge of the particular fraud case.

Employees not directly involved with a particular fraud case shall not have routine access to sensitive information. This shall include the following:

- Employees who are not part of the PSC or Medicare contractor BI unit.

- Corporate employees working outside the Medicare division.

- Clerical employees who are not integral parts of the PSC or Medicare contractor BI unit.

Employees should keep in mind that any party that is the subject of a fraud investigation is likely to use any means available to obtain information that could prejudice the investigation or the prosecution of the case. As previously noted and within the above exceptions, PSCs and Medicare contractor BI units shall not release information to any person outside of the PSC or Medicare contractor BI unit and law enforcement staff, including provider representatives and lawyers.

Although these parties may assert that certain information must be provided to them based on their “right to know,” PSCs and Medicare contractor BI units have no legal obligation to comply with such requests. The PSCs and Medicare contractor BI units shall request the caller's name, organization, and telephone number. Indicate that verification of whether or not the requested information is authorized for release must occur before response may be given. Before furnishing any information, however, PSCs and Medicare contractor BI units shall definitely determine that a caller has a “need to know,” and that furnishing the requested information will not prejudice the investigation or case or prove harmful in any other way. Each investigation and case file shall list the name, organization, address and telephone numbers of all persons with whom the PSC or

Medicare contractor BI unit can discuss the investigation or case (including those working within the PSC or Medicare contractor BI unit).

While PSC and Medicare contractor BI unit management may have access to general case information, it shall only request on a need-to-know basis specific information about investigations that the PSC or Medicare contractor BI unit is actively working.

The OIG shall be notified if parties without a need to know are asking inappropriate questions. The PSC and Medicare contractor BI unit shall refer all media questions to the CMS press office.

F - Computer Security

Access to BI information in computers shall be granted only to PSC or Medicare contractor BI unit employees. The following guidelines shall be followed:

- Employees shall comply with all parameters/standards in CMS' Information System Security Policy, Standards and Guidelines Handbook and with the System Security Plan (SSP) Methodology.

- Access to computer files containing information on current or past fraud investigations shall be given only to employees who need such access to perform their official duties.

- Passwords permitting access to BI compatible files or databases shall be kept at the level of confidentiality specified by the PSC or Medicare contractor BI unit supervisory staff. Employees entering their passwords shall ensure that it is done at a time and in a manner that prevents unauthorized persons from learning them.

- Computer files with sensitive information shall not be filed or backed up on the hard drive of personal computers, unless one of the two following exceptions are met: 1) the hard drive is a removable one that can be secured at night (the presumption is that a computer with a fixed hard drive is not secure); and 2) the computer can be protected (secured with a “boot” password, a password that is entered after the computer is turned on or powered on). This password prevents unauthorized users from accessing any information stored on the computer's local hard drive(s) (C drive, D drive).

- Another safe and efficient way to preserve data is to back it up. Backing up data is similar to copying it, except that back-up utilities compress the data so that less disk space is needed to store the files.

- Record sensitive information on specially marked floppy disks or CDs and control and file these in a secure container placed in a locked receptacle (desk drawer, file cabinet, etc.). Check computers used for sensitive correspondence to ensure that personnel are not filing or backing up files on the hard drive. The configuration of

the software needs to be checked before and after the computer is used to record sensitive information.

- Limit the storage of sensitive information in provider files with open access. Conclusions, summaries, and other data that indicate who will be indicted shall be in note form and not entered into open systems.

- The storage of sensitive information on a Local Area Network (LAN) or Wide Area Network (WAN) is permissible if the two following parameters are satisfied:

    1) The LAN/WAN shall be located on a secure Server and the LAN/WAN drive shall be mapped so that only staff from the BI unit have access to the part of the LAN in which the sensitive information is stored.

    2) LAN/WAN Administrators have access to all information located on the computer drives they administer, including those designated for the BI unit. As such, LAN/WAN Administrators shall also complete an annual confidentiality statement.

Environmental security measures shall also be taken as follows:

- Electronically recorded information shall be stored in a manner that provides protection from excessive dust and moisture and temperature extremes.

- Computers shall be protected from electrical surges and static electricity by installing power surge protectors.

- Computers shall be turned off if not being used for extended periods of time.

- Computers shall be protected from obvious physical hazards, such as excessive dust, moisture, extremes of temperature, and spillage of liquids and other destructive materials.

- Class C (electrical) fire extinguishers shall be readily available for use in case of computer fire.

G - Telephone Security

The PSC or Medicare contractor BI unit shall implement phone security practices. As stated earlier in this section, the PSC or Medicare contractor BI unit 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 or Medicare contractor BI unit involved in the investigation of the related issue.

This applies to persons unknown to the PSC or Medicare contractor BI unit who say they are with the FBI, OIG, DOJ, etc. The PSC or Medicare contractor BI unit shall only use CMS, OIG, DOJ, and FBI phone numbers that can be verified. Management shall provide PSC or Medicare contractor BI unit staff with a list of the names and telephone numbers of the individuals of the authorized agencies that the PSC or Medicare contractor BI unit 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. Personnel shall be cautious of callers who “demand” information and continue to question the PSC or Medicare contractor BI unit after it has stated that it is not at liberty to discuss the matter. Again, it is necessary to be polite, but firmly state that the information cannot be furnished at the present time and that the caller will have to be called back. PSCs and Medicare contractor BI units shall not respond to questions concerning any case being investigated by the OIG, FBI, or any other law enforcement agency. The PSCs and Medicare contractor BI units shall refer them to the OIG, FBI, etc., as appropriate.

PSCs and Medicare contractor BI units shall transmit sensitive information via facsimile (fax) lines only after it has been verified that the receiving fax machine is secure. Unless the fax machine is secure, PSCs or Medicare contractor BI units shall make arrangements with the addressee to have someone waiting at the receiving machine while the fax is being transmitted. Sensitive information via fax shall not be transmitted when it is necessary to use a delay feature, such as entering the information into the machine's memory.

4.4.1 - Requests for Information From Outside Organizations

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

Federal and state law enforcement agencies may seek information to further their investigations or prosecutions of individuals or businesses alleged to have committed fraud. PSCs and Medicare contractor BI units may share certain information 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 or Medicare contractor 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 Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Both the Privacy Act and the Privacy 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 or Medicare contractor BI unit. PSC and Medicare contractor BI unit questions concerning what information may be disclosed under the Privacy Act or Privacy Rule shall be directed to CMS 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. It 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.

The Privacy Act affords protection only to individuals. Therefore, there is a privacy issue only when the information pertains to specific persons, e.g., physicians or beneficiaries. In all cases, the PSC or Medicare contractor BI unit is free to share with law enforcement the nature of the scams or fraudulent schemes active in the area.

The Privacy Act and the HIPAA Privacy Rule protect information "records," which are maintained in "systems 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. The Federal Register *S*ystem of *R*ecords *notices* maintained by *CMS* may be found on the CMS Web site at http://cms.hhs.gov/privacy/tblsors.asp.

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.

A - Requests from Private, Non-Law Enforcement Agencies

Generally, PSCs and Medicare contractor 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, Medicare contractors shall contact the CMS RO for further direction. Similarly, PSCs shall contact their Government Task Leader (GTL), Co-GTL, and SME for any further guidance.

B - Requests from Medicare Contractors and Program Safeguard Contractors

PSCs and Medicare contractor BI units may furnish requested specific information on ongoing fraud investigations and on individually identifiable protected health information to any PSC, AC, or Medicare contractor BI unit. PSCs, ACs, and Medicare contractor BI units 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, PSCs or Medicare contractor BI units shall refer the requesting PSC or Medicare contractor BI unit to the OIG/OI.

C - Quality Improvement Organizations and State Survey and Certification Agencies

PSCs and Medicare contractor 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, PSCs and Medicare contractor BI units shall refer the requestor to the OIG/OI.

D - State Attorneys General and State Agencies

PSCs and Medicare contractor 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). See Section 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 §G below and PIM Exhibit 25 for guidance on how requests should be structured to comply with the Privacy Rule. PSCs and Medicare contractor 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, PSCs and Medicare contractor BI units shall refer the requestor to the OIG/OI.

E - Request from Medicaid Fraud Control Units

Under current Privacy Act requirements applicable to program integrity investigations, PSCs and Medicare contractor 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 Section 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 §G below and PIM Exhibit 25 for guidance on how requests should be structured to comply with the Privacy Rule. PSCs and Medicare contractor 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, PSCs and Medicare contractor BI units shall refer the requestor to the OIG/OI.

F - Requests from OIG/OI for Data and Other Records

PSCs and Medicare contractor BI units shall provide the OIG/OI with requested information, and shall maintain cost information related to fulfilling these requests. If major/costly systems enhancements are required to fulfill a request, the PSCs shall discuss the request with the GTL, Co-GTL, and SME before fulfilling the request, and the Medicare contractor BI units shall discuss the request and the cost with the RO 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's or Medicare contractor BI unit's files. Based on review of its available resources, the PSC or Medicare contractor BI unit shall inform the requestor what, if any, portion of the request can be provided. The PSC or Medicare contractor BI unit shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested.

PSCs and Medicare contractors BI units shall respond to such requests within 30 days whenever possible. If that timeframe cannot be met, the PSC or Medicare contractor BI unit shall notify the requesting office as soon as possible (but not later than 30 days) after receiving the request. PSCs and Medicare contractor *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.

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 or Medicare contractor BI unit shall inform the requestor what, if any, portion of the request can be provided. The PSC or Medicare contractor BI unit shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested.

PSCs and Medicare contractor BI units shall respond to such requests within 45 calendar days, when possible. If that timeframe cannot be met, the PSC or Medicare contractor BI unit shall notify the requesting office within the 45-day timeframe, and include an estimate of when all requested information will be supplied. This timeframe applies to all requests with the exception of those that require DESY access to NCH.

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, Federal Agreement (Office of Inspector General) for Release of Data with Individual Identifiers (see Exhibit 37). To comply with the Privacy Rule, the paragraph below should be added to the form. If the OIG/OI requests protected health information that is not in a data format, e.g., copies of medical records that the PSC has in its possession, the OIG/OI should include the paragraph in its written request for the information.

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 GTL, Co-GTL, and SME. The Medicare contractor BI unit shall contact the RO.

G – 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 and Medicare contractor BI units) 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.

PIM Exhibit 25 contains the entire document issued by the DOJ on April 11, 2003. PSCs and Medicare contractor 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, FBI agents, AUSAs, paralegals, analysts and/or investigators). 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; 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, 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.

As part of the initial consultation process, the PSC or Medicare contractor BI unit and law enforcement agency shall develop appropriate language to insert in the data request form letter, including:

- Type of data and data elements needed.

- Name and/or other identifying information for provider(s) (e.g., Tax Identification Number, Unique Physician Identification Number, etc.).

- Time period of data to be reviewed (approximate begin and end dates if the conduct is not ongoing currently).

- Preferred format or medium for data to be provided (i.e., tape, CD-ROM, paper, etc.).

Once the language is formulated, 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 described above, to the PSC or Medicare contractor 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, 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 Blvd.
Baltimore, MD. 21244

Upon receiving a data request from DOJ, the PSC or Medicare contractor BI unit shall examine its sources of data for the most recent 36-month period for the substantive matter(s) in question or for the specific period requested by the DOJ, if necessary. Based on the review of its available data resources, the PSC or Medicare contractor BI unit shall inform the requestor what, if any, portion of the data can be provided. The PSC or Medicare contractor BI unit shall provide the relevant data, reports and findings to the requestor in the format(s) requested within 30 days when data for the most recent 36-month period is being sought directly from the PSC or Medicare contractor BI unit. If it is necessary for the PSC or Medicare contractor BI unit to seek and acquire data from CMS or another affiliated Medicare contractor, the time period required to provide the data to the requesting agency will extend beyond 30 days.

If appropriate, the PSC or Medicare contractor BI unit shall also use available analytic tools to look for other possible indicia of fraud in addition to the specific alleged conduct that was the cause of the DOJ data request.

If, in the view of the requesting DOJ, the PSC, the Medicare contractor BI unit, or CMS, the initial 36-month review generally verifies the fraud allegations, or if potential fraud is uncovered through the use of analytic tools, the PSC or Medicare contractor BI unit shall conduct a supplemental review of Medicare data if it receives a subsequent request. The supplemental review will meet the specific needs of the DOJ based on the allegations under investigation and/or findings of the initial 36-month review. Such supplemental reviews may involve retrieving information from original Carrier and/or Fiscal Intermediary data files, the National Claims History (NCH), the Common Working File

(CWF), or other Medicare data files that may be archived, in order to cover the complete time frame involved in the allegations and/or allowed by the statute of limitations.

Every effort shall be made to fulfill all data requests within the time constraints faced by the DOJ. It may be necessary to negotiate a time period for fulfilling supplemental data requests on a case-by-case basis with the requestor when the scope of the request exceeds resources and/or current workload.

While the previous steps describe the usual process to be followed for handling DOJ requests for CMS Medicare data, exceptions to this process may be necessary on a case-by-case basis when the DOJ determines that conducting an initial review of the most recent 36 months of data would not be sufficient. For example, exceptions may be necessary if:

- The most recent 36 months of data would not be helpful to the investigation because the fraud being investigated is alleged to have occurred prior, or in large part prior to, that period.

- Changes in the payment system used for the type(s) of claims in question cause the most current data to be inappropriate for attempting to verify allegations of possible fraud that occurred under a previous payment system.

- The purpose of the data request cannot be met using only the most recent 36 months of data (e.g., a statistical sampling plan that requires more than 36 months of data to implement the plan correctly and accurately).

- Litigation deadlines preclude conducting an initial review followed by a more comprehensive supplemental review.

The prior items are illustrative, not exhaustive.

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 PSCs and Medicare contractor BI units may not have sufficient money in their budgets to respond to DOJ requests. In such cases, Medicare contractor BI units are advised to submit to CMS a Supplementary Budget Request (SBR). PSCs shall contact their GTLs, Co-GTLs, and SMEs.

To facilitate CMS' ability to track the frequency and burden of DOJ requests, the Medicare contractor BI unit shall maintain and submit to CMS, on a quarterly basis, a log of DOJ data requests that has been itemized to show costs for filling each request. This

report should be in the form of an Excel spreadsheet (see PIM Exhibit 26) and shall include, at a minimum, the following fields:

1. Medicare contractor name and identification number

2. Date of DOJ request

3. Nature of DOJ request and DOJ tracking number, if provided

4. Cost to fulfill request

5. Medicare contractor's capacity to fill request, including date of SBR submission, if necessary

The report shall be sent to the following address:

Director, Division of Benefit Integrity and Law Enforcement Liaison
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Mail Stop C3-02-16
Baltimore, Maryland 21244

H - Law Enforcement Requests for Medical Review

PSCs and Medicare contractor 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 or Medicare contractor BI unit to review and interpret medical records for them, the PSC and Medicare contractor 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 dates

- Format required for response

The PSC shall present the written request to the GTL, Co-GTL, and SME and the Medicare contractor BI unit shall present the written request to their RO prior to fulfilling the request. Each written request will be considered on a case-by-case basis to determine whether the request will be approved.

I – 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 and Law Enforcement Liaison 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.

J - 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.* PSC*s* shall refer requests that raise Privacy Act concerns and/or issues to the GTL, Co-GTL, and SME for further consideration, and Medicare contractor BI units shall refer requests to their CMS RO.

K – 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 or Medicare contractor BI unit receives duplicate requests for information, the PSC or Medicare contractor BI unit shall notify the requestors. If the requestors are not willing to change their requests, the PSC or Medicare contractor BI unit shall ask the GTL, Co-GTL, and SME (if a PSC) or CMS RO employee (if a Medicare contractor BI unit) for assistance.

L - Reporting Requirements

For each data request received from DOJ, PSCs and Medicare contractor 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 RO, GTL, Co-GTL, or SME had to intervene on the outcome (request fulfilled or not fulfilled)

- The cost of furnishing a response to each request

The Medicare contractor shall report the data to the RO when requested by the RO. This data will be used to assess budget requirements.

4.4.2 - Program Safeguard Contractor and Medicare Contractor Coordination with Other Program Safeguard Contractors and Medicare Contractors

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

PSCs and Medicare contractor BI units shall coordinate with other PSCs and Medicare contractor 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 or Medicare contractor BI units. Coordination is also necessary because certain findings of fraud involving a provider could have a direct effect on payments made by ACs or Medicare contractors. PSCs and Medicare contractors use the appropriate staff member(s) to share information with Medicare contractors not in contiguous states.

4.6.2 - Complaint Screening

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

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

A - Medicare Contractor and Affiliated Contractor Responsibilities

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

Initial Screening

Customer service representatives (CSRs) shall try to resolve as many inquiries as possible in the Initial Screening with data available in their desktop system. The CSRs shall send an acknowledgement or resolution letter for written requests within 45 calendar days of the receipt date stamped in the mailroom, unless the written request can be acknowledged or resolved over the telephone. 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, etc.). 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.

Initial Screening activities shall be charged to Activity Code 13002 (Beneficiary and Provider Written Inquiries), Activity Code 13003 (Beneficiary and Provider Walk-in Inquiries), Activity Code 13005 (Beneficiary Telephone Inquiries), or Activity Code 33001 (Provider Telephone Inquiries), whichever is the most applicable. In fiscal year 2004, there is a separate Activity Code for Provider Written Inquiries (33002) and Provider Walk-in inquiries (33003). The current Beneficiary Inquiries Manual Instructions will be revised and the FY2004 Budget and Performance Requirements will be developed to reflect the following Performance Priorities: 1) Telephones, 2) Second Level Screening, 3) Written, and 4) Walk-in, and 5) Customer Service Plan Activities.

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 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 for handling.

The initial screening staff shall maintain a log of all potential fraud and abuse inquiries. At a minimum, the log shall contain the following information:

- Beneficiary name
- Provider Name
- Beneficiary HIC#
- Nature of the Inquiry
- Date of the Inquiry
- Internal Tracking Number
- Date Referred to the Second Level Screening Staff
- Date Closed

Second-Level Screening

When the complaint/inquiry cannot be resolved by the CSR, the issue shall be referred for more detailed screening, resolution, or referral, as appropriate, within the AC or Medicare contractor. If the second level screening staff is able to resolve the inquiry without referral, they shall send a resolution letter, unless it can be resolved by telephone, within 45 calendar days of receipt from the initial screening staff, or within 30 calendar of receiving medical records and/or other documentation, whichever is later. The second-level screening staff 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 forwarded to the Medicare contractor BI unit or the date it is sent to the PSC

- Destination of the referral (i.e., name of PSC or Medicare contractor BI unit)

- Documentation that an inquiry received from the initial screening staff was not forwarded to the PSC or Medicare Contractor 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 Medicare contractor 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 Medicare contractor shall request and review certain documents, as appropriate, from the provider, such as itemized billing statements and other pertinent information. If the AC or Medicare contractor 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 Medicare contractor 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 calendar 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 or Medicare contractor BIU)*. 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 is suspected after performing the billing and document review, the medical record shall be forwarded to the PSC (if BI work was transitioned to a PSC) or Medicare contractor BI unit for clinician review. If the AC or Medicare contractor 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. In these instances, the AC or Medicare contractor shall also be responsible for acknowledging these complaints, and sending appropriate resolution letters to the beneficiary or complainant. If the AC or Medicare contractor 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 or Medicare contractor BI unit for further development within 45 calendar days of the date of receipt from the initial screening staff, or within 30 calendar days of receiving medical records and/or other documentation, whichever is later. The AC or Medicare contractor 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 or Medicare contractor BI unit for further development.

The AC or Medicare contractor shall be responsible for screening all Harkin Grantee complaints for fraud. If after conducting second level screening, the AC or Medicare contractor staff determines that the complaint is a potential fraud and abuse situation, the complaint shall be sent to the PSC or Medicare contractor BI unit within 45 calendar days

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

The AC or Medicare contractor 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 Medicare contractor determines that the complaint is a potential fraud and abuse situation, the second-level screening staff shall forward it to the PSC or Medicare contractor BI unit for further development within 45 calendar days of receipt, or within 30 calendar days of receiving medical records and/or other documentation, whichever is later, just like all other complaints. The PSC or Medicare contractor BI unit shall be responsible for updating the valid cases that have been referred. PSCs and Medicare contractors 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 and Medicare contractors shall refer to this number in all correspondence to the RO.

Complaints shall be forwarded to the Medicare contractor BI unit or PSC 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 two 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 Medicare contractor 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 or Medicare contractor BI unit for further development, the AC or Medicare contractor 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 Medicare contractor'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 Medicare contractor employee who received the complaint.

NOTE: Since this is not an all-inclusive list, the PSC or Medicare contractor 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 or Medicare contractor 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 Medicare contractor employee who received the complaint.

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

The AC or Medicare contractor 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 open *and* closed (report the same complaint only once) in workload column 1; report the total number of medical records ordered for beneficiary inquiries that were open *and* closed (report the same complaint only once) in workload column 2; and report the total number of potential fraud and abuse beneficiary complaints identified and referred to the PSC or Medicare contractor BI unit in workload column 3. The AC or Medicare contractor shall keep a record of the cost and workload for all provider inquiries of potential fraud and abuse that are referred to the PSC or Medicare contractor BI unit in Activity Code 13201/01.

NOTE: *The same complaint shall only be counted once in the same month. However, it is possible that the same complaint will be counted more than once from month to month (e.g., counted as opened in October; pending in November; and closed in December). Open indicates any complaints opened and pending in the reporting month.*

B – Program Safeguard Contractor and Medicare Contractor Benefit Integrity Unit Responsibilities

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

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

If the PSC or Medicare contractor 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, etc.), it shall be referred to the AC or Medicare contractor area responsible for second-level screening, or if applicable, the appropriate PSC unit for further action. This shall allow the AC or Medicare contractor screening area to track the complaints returned by the PSC or Medicare contractor BI unit. However, the PSC or Medicare contractor BI unit shall send an acknowledgement to the complainant, but indicate that a referral is being made, if applicable, to the appropriate PSC, or to the appropriate AC or Medicare contractor unit for further action.

The PSC or Medicare contractor BI unit shall be responsible for communicating any updates as a result of their investigation on Harkin Grantee complaints to the AC or Medicare contractor second-level screening staff, who shall update the database accordingly.

The PSC or Medicare contractor BI unit shall be responsible for updating valid cases that have been referred from the OIG Hotline Database by the AC or Medicare contractor second-level screening area.

The PSC or Medicare contractor BI unit shall be responsible for sending the complainant a resolution within 7 calendar days of the resolution on the complaint investigation and/or case in accordance with PIM Chapter 4, §4.8.

4.10.1 - Types of Fraud Alerts

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

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 CMS 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 or Medicare contractor BI unit 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. *Medicare contractor BI units* and PSCs shall distribute Alerts to all agencies in their jurisdiction within 15 working days of receipt by the PSC or Medicare contractor BI unit.

Draft National Medicare Fraud Alerts to CO shall be password protected and emailed to the CMS CO Director of the Division of Benefit Integrity and Law Enforcement Liaison.

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

> **Distribution of this Fraud Alert is Limited to the Following Audience:**
>
> **CMS Regional Offices, *Medicare Contractor* Benefit Integrity Units, 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 *Medicare contractors BI units* and/or PSCs. However, if the *Medicare contractor BI units* or 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

CMS issues an RMFA when specific providers are identified as being suspected of engaging in fraudulent or abusive practices or activities. PSCs and Medicare contractor BI units prepare this type of Alert (see PIM Exhibit 28 for the RMFA template) when advising other Medicare carriers, intermediaries, 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, Medicare contractors, CMS, QIOs, OIG/OI, DCIS, FBI, MFCUs, U.S. Postal Service, IRS, and the Offices of the U.S. Attorney. The CMS CO will issue each *Medicare contractor BI unit and PSC* one copy of an RMFA along with a sanitized version. Each *Medicare contractor BI unit* and PSC 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 or Medicare contractor BI unit.

Draft Restricted Medicare Fraud Alerts shall be emailed password protected via the secure email system. If problems occur with the secure email system, RMFAs shall be mailed to the following address:

> Centers for Medicare & Medicaid Services
> OFM/PIG/DBIL
> 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:

Centers for Medicare & Medicaid Services Regional Offices, *Medicare Contractor* Benefit Integrity Units, 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: *RMFAs will be distributed to Medicare Integrity Program Units on a need to know basis.*

C - CMS Central Office Alert

PSCs and Medicare contractor BI units shall prepare a CMS CO Alert when:

- PSCs or Medicare contractor 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 and Law Enforcement Liaison (DBILEL) Director, the CMS CO PIG Director, the CMS CO PIG Deputy Director, and the CMS CO Fraud Alert Lead.

D – Program Safeguard Contractor or Medicare *Contractor BI Unit* Alert

- Initially, this Alert generally is sent to the CMS 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.
- CMS notifies the PSC or *Medicare contractor BI unit* of the Alert denial.

- If the PSC and *Medicare contractor BI unit* do not provide CMS with any additional information to justify reconsideration, the denial is final. However, the *PSC and Medicare Contractor BI Unit* may issue denied Alerts as PSC/*Medicare Contractor BI Unit* Alerts.

- The PSC and *Medicare contractor BI unit* shall provide the CMS 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 PSCs and Medicare contractor 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, PSCs and Medicare contractor BI units shall provide this information to their respective ACs or Medicare contractor unit 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. PSCs and Medicare contractor BI units shall also monitor the MED for consistency.

4.10.2 - Alert Specifications

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

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 or *Medicare Contractor 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., PIM, Medicare Carrier Manual (MCM), Medicare Intermediary Manual (MIM) section, National Coverage Determinations (NCD), LMRP, 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 or Medicare contractor 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 PSCs or Medicare contractor 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/*Medicare contractor 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, Medicare contractors, and federal law enforcement agencies. Restricted Alerts shall not be distributed beyond the approved distribution list.

4.10.3 - Editorial Requirements

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

PSCs and Medicare contractor 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. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

Before preparing an Alert, the PSC or *Medicare contractor BI unit* shall consult with the applicable CMS RO and/or, PSC network, GTL, Co-GTL, SME, and Medicare contractor BI unit manager. The PSC or *Medicare contractor BI unit* shall determine whether or not a similar Alert has been issued by contacting PSCs *or Medicare contractor 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 and *Medicare contractor BI unit* shall forward the draft to CMS Program Integrity Group or the GTL, Co-GTL, and SME (if a PSC) for review and clearance. The Program Integrity Group reviews the draft, acknowledges the Alert, and notifies the PSC or Medicare contractor 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 or *Medicare contractor BI unit* Alert

The CMS CO keeps the PSC or *Medicare contractor BI unit* informed of the progress of the Alert throughout the clearance process.

4.10.5 - Distribution of Alerts

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

The CMS issues the Alert to the PSCs or *Medicare contractor 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 or *Medicare contractor 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. PSCs or *Medicare contractor BI units* shall distribute the Alert to the entities that appear on the audience line.

4.11.1 - Background

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

The FID shall capture information on investigations that have been initiated by the PSC or Medicare contractor BI unit and on cases that have been referred to law enforcement by the PSC or Medicare contractor BI unit. The FID shall also capture information on payment suspensions that have been imposed.

Investigations initiated by the PSC or Medicare contractor BI unit shall be saved in the FID, and contain identifying information on the potential subject of a case.

Cases initiated by the PSC or Medicare contractor 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, etc.).
- Allegation information/nature of the scheme.
- Status of the case.
- Disposition of a case (e.g., administrative action, prosecution, exclusion, settlement, etc.).
- Contact information for PSC, Medicare contractor 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 PSCs, Medicare contractor 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. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

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

4.11.2.1 - Initial Entry Requirements for Investigations

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

Investigations shall capture information on ongoing work in the PSC or Medicare contractor BI unit. For PSCs, investigations are entered when they are reported on the PSC's ART report. For Medicare contractor BI units, investigations are entered when they are being worked in the BI unit, regardless of level of effort, but have not been referred to law enforcement as a case.

Investigations initiated by the PSC or Medicare contractor 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). Such 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 Medicare contractor 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 or Medicare contractor BI unit initiated investigations)

CONTACTS Tab:

[Confirm contact information is accurate]

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

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

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)
The *designated PSC and Medicare contractor 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 PSCs and Medicare contractor BI units and law enforcement personnel within their jurisdiction.

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

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

4.16 – *AC and PSC Coordination on Voluntary Refunds*

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

Voluntary refund checks payable to the Medicare program shall not be returned, regardless of the amount of the refund. The PSC or Medicare contractor BI unit shall communicate with the AC or Medicare contractor staff responsible for processing voluntary refunds to obtain information on voluntary refund checks received. The PSC or Medicare contractor 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 or Medicare contractor BI unit receive a voluntary refund check in error, the PSC shall coordinate the transfer of voluntary refund checks to the AC through the JOA, and the Medicare contractor BI unit shall transfer the check to the appropriate Medicare contractor staff. For PSCs, voluntary refund checks shall be processed and deposited by the AC.

ACs and the appropriate Medicare contractor staff refer to the Financial Management Manual for instructions on processing and reporting unsolicited/voluntary refunds received from providers/physicians/suppliers and other entities.

Through the JOA, PSCs shall establish a mechanism whereby the AC notifies the PSC on a regular basis of all voluntary *refunds* received by the AC. Medicare contractor BI units shall work with the appropriate area in the Medicare contractor to receive such notification. PSCs and Medicare contractor BI units shall send one letter annually *(calendar year)* to the same provider submitting a voluntary refund, 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.

PSCs shall advise providers to send voluntary *refunds* to the AC.

4.17 – *Reserved for Future Use*

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

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

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

PSCs and Medicare contractor 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 or Medicare contractor 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 actual 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 or Medicare contractor BI unit does not hear from OIG/OI within the first 90 calendar days following referral, and repeated attempts by the PSC or Medicare contractor BI unit to find out the status of the case are unsuccessful, the PSC or Medicare contractor BI unit shall *contact* the FBI *(if the FBI does not have the case referral, the PSC and Medicare contractor 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 or Medicare contractor 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, contact the GTL, Co-GTL, and SME (if a PSC) or RO (if a Medicare contractor BI unit) 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 GTL/Co-GTL/SME or RO, PSCs and Medicare contractor BI units shall proceed with action to ensure the integrity of the Medicare Trust Fund (e.g., PSCs and Medicare contractor BI units shall discuss it with the AUSA and/or the OIG prior to taking administrative action).

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 or Medicare contractor BI unit for administrative action/recovery of overpayment with no further investigation
- Refer the case back to the PSC or Medicare contractor 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 or Medicare contractor 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 or Medicare contractor BI unit to establish evidence (i.e., data summaries, statements, bulletins, etc.) that a statutory violation has occurred.

In addition to referral of such cases to the OIG, PSCs and Medicare contractor 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. PSCs and Medicare contractor 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 or Medicare contractor 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 or Medicare contractor BI unit against taking administrative action, the PSC shall contact the GTL, Co-GTL, and SME and the Medicare contractor shall contact the RO. The GTL, Co-GTL, and SME for a PSC and the RO for a Medicare contractor will decide whether or not to take administrative action.

It is important to alert 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.

If the case is the focus of a national investigation, PSCs and Medicare contractor BI units shall not take action without first consulting with the GTL, Co-GTL, and SME (if a PSC) or the RO (if a Medicare contractor BI unit), and the agency that has the lead for the investigation.

4.18.2 - Referral to State Agencies or Other Organizations

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)
PSCs and Medicare contractor 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, PSCs and Medicare contractor 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, PSCs Medicare contractor 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 GTLs, Co-GTLs, and SMEs, and Medicare contractor BI units shall work closely with their RO BI coordinator on these referrals. The BI coordinator shall involve the necessary staff in CMS.

Concurrently, PSCs or Medicare contractor 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. PSCs or Medicare contractor 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

4.20.2.2 - Civil Monetary Penalties Delegated to OIG

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

The following is a brief description of authorities from the Social Security Act:

Section 1128(a)(1)(A), (B)	False or fraudulent claim for item or service including incorrect coding (upcoding) or medically unnecessary services.
Section 1128A(a)(1)(C)	Falsely certified specialty.
Section 1128A(a)(1)(D)	Claims presented by excluded party.
Section 1128A(a)(1)(E)	Pattern of claims for unnecessary services or supplies.
Section 1128A(a)(2)	Assignment agreement, Prospective Payment System (PPS) abuse violations.
Section 1128A(a)(3)	PPS false/misleading information influencing discharge decision.
Section 1128A(a)(4)	Excluded party retaining ownership or controlling interest in participating entity.
Section 1128A(a)(5)	Remuneration offered to induce program beneficiaries to use particular providers, practitioners, or suppliers.
Section 1128A(a)(6)	Contracting with an excluded individual.
Section 1128A(a)(7)	Improper remuneration; i.e., kickbacks.
Section 1128A(b)	Hospital physician incentive plans.
Section 1128A(b)(3)	Physician falsely certifying medical necessity for home health benefits.
Section 1128E(b)	Failure to supply information on adverse action to the Health Integrity and Protection Data Bank (HIPDB).
Section 1140(b)(1)	Misuse of Departmental symbols/emblems.
Section 1819(b)(3)(B) Section 1919(b)(3)(B)	False statement in assessment of functional capacity of skilled nursing facility (SNF) resident.
Section 1819(g)(2)(A) Section 1919 (g)(2)(A)	Notice to SNF/nursing facility of standard scheduled survey.

Section 1857(g)(1)(F)	Managed care organization (MCO) fails to comply with requirements of §1852(j)(3) or §1852(k)(2)(A)(ii). (Prohibits MCO interference with the provider's advice to an enrollee; mandates that providers not affiliated with the MCO may not bill or collect in excess of the limiting charge.)
Section 1860D-31(i)(3)	*Engaged in false or misleading marketing practices under the Medicare prescription drug discount card program; or overcharge prescription drug enrollees; or misuse of transitional assistance funds.*
Section 1862(b)(3)(c)	Financial incentives not to enroll in a group health plan.
Section 1866(g)	Unbundling outpatient hospital costs.
Section 1867	Dumping by hospital/responsible physician of patients needing emergency medical care.
Section 1876(i)(6)(A)(i) Section 1903(m)(5)(A)(i) Section 1857(g)(1)(A)	Failure by Health Maintenance Organization (HMO)/competitive medical plan/MCO to provide necessary care affecting beneficiaries.
Section 1876(i)(6)(A)(ii) Section 1903(m)(5)(A)(ii) Section 1857(g)(1)(B)	Premiums by HMO/competitive medical plan/MCO in excess of permitted amounts.
Section 1876(i)(6)(A)(iii) Section 1903(m)(5)(A)(iii) Section 1857(g)(1)(C)	HMO/competitive medical plan/MCO expulsion/refusal to re-enroll individual per prescribed conditions.
Section 1876(i)(6)(A)(iv) Section 1903(m)(5)(A)(iii) Section 1857(g)(1)(D)	HMO/competitive medial plan/MCO practices to discourage enrollment of individuals.
Section 1876(i)(6)(A)(v) Section 1903(m)(5)(A)(iii) Section 1857(g)(1)(E)	False or misrepresenting HMO/competitive medical plan/MCO information to Secretary.
Section 1876(i)(6)(A)(vi) Section 1903(m)(5)(A)(v) Section 1857(f)	Failure by HMO/competitive medical plan/MCO to assure prompt payment for Medicare risk-sharing contracts only or incentive plan provisions.
Section 1876(i)(6)(A)(vii) Section 1857(g)(1)(G)	HMO/competitive medical plan/MCO hiring/employing person excluded under §1128 or §1128A.

Section 1877(g)(3)	Ownership restrictions for billing clinical lab services.
Section 1877(g)(4)	Circumventing ownership restriction governing clinical labs and referring physicians.
Section 1882(d)(1)	Material misrepresentation referencing compliance of Medicare supplemental policies (including Medicare + Choice).
Section 1882(d)(2)	Selling Medicare supplemental policy (including Medicare + Choice) under false pretense.
Section 1882(d)(3)(A)	Selling health insurance that duplicates benefits.
Section 1882(d)(3)(B)	Selling or issuing Medicare supplemental policy (including Medicare + Choice) to a beneficiary without obtaining a written statement from beneficiary with regard to Medicaid status.
Section 1882(d)(4)(A)	Use of mailings in the sale of non-approved Medicare supplemental insurance (including Medicare + Choice).
Section 1891(c)(1)	Notifying home health agency of scheduled survey.
Section 1927(b)(3)(B)	False information on drug manufacturer survey from manufacturer/wholesaler/seller.
Section 1927(b)(3)(C)	Provision of untimely or false information by drug manufacturer with rebate agreement.
Section 1929(i)(3)	Notifying home- and community-based care providers/settings of survey.
Section 421(c) of the Health Care Quality Improvement Act (HCQIA)	Failure to report medical malpractice liability to National Practitioner Data Bank.
Section 427(b) of HCQIA	Breaching confidentiality of information report to National Practitioner Data Bank.

4.27 - Annual Deceased-Beneficiary Postpayment Review

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

The PSCs and Medicare contractor 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, starting fiscal year 2003, for beneficiaries who died the previous fiscal year. In addition, the PSCs shall forward the identified overpayments to the AC 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 - PSCs and Medicare contractor BI units must identify improperly paid services. Upon identification, PSCs and Medicare contractors will refer this information to their respective AC or appropriate area within the Medicare contractor for recoupment. ACs and Medicare contractors must issue associated overpayment demand letters as soon as administratively possible.

PSCs, ACs, and Medicare contractors are not required to perform medical review for paid claims with dates of service after a beneficiary's date of death. PSCs and Medicare contractor 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 appropriate area within the Medicare contractor. 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 Medicare contractor.

At a minimum, PSCs and Medicare contractor 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's or Medicare contractor 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, PSCs and Medicare contractor 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 PSCs and Medicare contractor BI units to utilize a CMS-created annual computer file of all deceased beneficiaries. On an annual calendar year basis, CMS creates a computer file of all Medicare beneficiaries who died in the preceding calendar year. This computer file should be available for PSCs and Medicare contractor BI

units to download from the CMS Data Center by mid-February of each year. PSCs and Medicare contractor BI units then review the format for this file to determine if any changes have been made from the previous fiscal year file. 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, PSCs and Medicare contractor 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 and Medicare contractor BI unit shall submit the name of the person(s) who will be accessing the files, their CMS mainframe user identification number, the PSC or Medicare contractor 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 email to the CMS CO Director of the Division of Benefit Integrity and Law Enforcement Liaison.

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 PSCs and Medicare contractor 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 PSCs and Medicare contractor BI units may consider developing an investigation on providers whose pattern of billings remains noncompliant.

On an annual basis, PSCs and Medicare contractor BI units shall submit a report to the on the accounting of the improper payments identified by the PSC or Medicare contractor BI unit and respective overpayments recouped by the AC and Medicare contractor. This report shall be due on December 5th of each year and sent to the GTL, Co-GTL, and SME. The report shall also be sent to the following address:

Director of the Division of Benefit Integrity and Law Enforcement Liaison
Centers for Medicare & Medicaid Services
Re: Deceased Beneficiaries
Mail Stop C3-02-16
7500 Security Boulevard
Baltimore, Maryland 21244

4.31 – Vulnerability Report

(Rev. 101, Issued: 01-28-05, Effective: 02-28-05, Implementation: 02-28-05)

Program vulnerabilities can be identified through a variety of sources such as the Chief Financial Officer's (CFO) Audit, Fraud Alerts, the General Accounting Office (GAO), the Office of Inspector General (OIG), and PSC and Medicare contractor operations, as examples. PSCs and Medicare contractor BI units shall submit any identified program vulnerabilities to CMS 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 and Medicare contractor BI unit shall send a copy of the identified vulnerabilities to the GTL, Co-GTL, and RO. The PSC and Medicare contractor BI unit shall also send the CMS CO a copy of the identified vulnerabilities to the following address: **vulnerability@cms.hhs.gov**