CMS Manual System

Pub. 100-08 Medicare Program Integrity

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

Transmittal 83 **Date: AUGUST 27, 2004**

CHANGE REQUEST 3379

SUBJECT: PIM Revisions for Chapter 4

I. SUMMARY OF CHANGES: This instruction revises and clarifies various sections of PIM Chapter 4.

NEW/REVISED MATERIAL - EFFECTIVE DATE: September 27, 2004
***IMPLEMENTATION DATE: September 27, 2004**

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

II. CHANGES IN MANUAL INSTRUCTIONS:
(R = REVISED, N = NEW, D = DELETED)

R/N/D	CHAPTER/SECTION/SUBSECTION/TITLE
R	4/4.2.2/Program Safeguard Contractor and Medicare Contractor Benefit Integrity Unit
R	4/4.2.2.6/Benefit Integrity Security Requirements
R	4/4.3/Medical Review for Benefit Integrity Purposes
R	4/4.4.1/Requests for Information from Outside Organizations
R	4/4.7.1/Conducting Investigations
R	4/4.8/Disposition of Cases
R	4/4.10.1/Types of Fraud Alerts
R	4/4.11.1/Background
R	4/4.11.2/Investigation, Case, and Suspension Entries
R	4/4.11.2.1/Initial Entry Requirements for Investigations
R	4/4.11.2.8/Closing Investigations
R	4/4.18.1/Referral of Cases to the Office of the Inspector General/Office of Investigations
R	4/4.18.1.3.1/Suspension
R	4/4.18.3/Referral to Quality Improvement Organizations
R	4/4.26.2/Exceptions

***III. FUNDING:**
These instructions shall be implemented within your current operating budget.

IV. ATTACHMENTS:

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

***Medicare contractors only**

Attachment – Business Requirements

Pub. 100-08	Transmittal: 83	Date: August 27, 2004	Change Request 3379

SUBJECT: PIM Revisions for Chapter 4

I. GENERAL INFORMATION

A. Background: Various sections of the PIM, Chapter 4 have been 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 #	Requirements	Responsibility
3379.1	The prohibition against hiring non-citizens was removed. Non-citizens may be hired in the BI unit after performing the thorough background and character reference checks specified in PIM, Chapter 4, §4.2.2.6D.	PSCs and Medicare contractor BI units
3379.2	PSCs shall follow Chapter 2, §2.3 for sources of data as specified in Chapter 4, §4.3.	PSCs
3379.3	Section 4.4.1G was revised to clarify that PSCs and Medicare contractor BI units shall fulfill data requests received from those individuals at FBI and DOJ who are involved in the work of the health care oversight agency (including, for example, FBI agents, AUSAs, paralegals, analysts, and/or investigators) in accordance with the guidelines in this section.	PSCs and Medicare contractor BI units
3379.4	PSCs and Medicare contractor BI units shall refer to Chapter 3, §3.8ff for overpayments as specified in Chapter 4, §4.7.1.	PSCs and Medicare contractor BI units
3379.5	When law enforcement requests that an investigation be referred before completion	PSCs and Medicare contractor BI units

	of the PSC's or Medicare contractor BI unit's investigation, PSCs and Medicare contractor BI units shall request law enforcement to send a letter or e-mail to them acknowledging that the PSC or Medicare contractor BI unit did not complete their investigation.	
3379.6	The PSCs and Medicare contractor BI units shall continue their investigation even though an expedited referral has been made to law enforcement in order to determine the appropriate administrative actions.	PSCs and Medicare contractor BI units
3379.7	Business requirements for Fraud Alerts have not changed for §4.10.1, but a typographical error was corrected.	PSCs and Medicare contractor BI units
3379.8	All references to law enforcement initiated investigations, cases, and data requests have been removed from the FID sections of the PIM, since the FID does not currently have this capability.	PSCs and Medicare Contractor BI units
3379.9	Within 60 days of identifying the necessity for administrative actions, the PSC and Medicare contractor BI unit shall consult with law enforcement prior to taking administrative action.	PSCs and Medicare contractor BI units.
3379.10	PSCs and Medicare contractor BI units shall continue to monitor the need for administrative action prior to the elapsing of the 90 days and consult with OIG or other law enforcement agencies before taking such measures.	PSCs and Medicare contractor BI units
3379.11	PSCs and Medicare contractor BI units shall refer to Chapter 3, §3.9ff for suspension of payment instructions.	PSCs and Medicare contractor BI units
3379.12	The PSC shall coordinate the review of Part A acute care inpatient hospital claims and long term care claims (i.e., long term acute care, not SNFs) for benefit integrity purposes with the QIO.	PSCs
3379.13	If the PSC investigation indicates a need to review Part A acute care inpatient PPS hospital medical records or long term care medical records, the PSC shall request the medical records directly from the provider and have them sent directly to the PSC.	PSCs
3379.14	Following the PSC review of the Part A	PSCs

	acute care inpatient PPS hospital claims or long term care claims and medical records, if the PSC determines that no potential fraud and abuse has been committed, or if the PSC determines that potential fraud and abuse is likely but law enforcement rejects the case, the PSC shall refer the provider and medical records back to the QIO for further medical review, provider education, or the initiation of overpayment calculation, payment determination, and overpayment request.	
3379.15	If after the PSC reviews the Part A acute care inpatient PPS hospital claims or long term care claims and medical records, the PSC determines that potential fraud and abuse is likely, the PSC shall coordinate the case with law enforcement (per Law Enforcement Memorandum of Understanding).	PSCs
3379.16	The supplier shall bill the date of service on the claim as the date of discharge and shall use the Place of Service (POS) as 12 (Patient's Home).	DMERCs

II. SUPPORTING INFORMATION AND POSSIBLE DESIGN CONSIDERATIONS

A. Other Instructions: N/A

X-Ref Requirements #	Instructions

B. Design Considerations: N/A

X-Ref Requirements #	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: September 27, 2004 **Implementation Date:** September 27, 2004 **Pre-Implementation Contact(s):** Kimberly Downin kdownin@cms.hhs.gov 410-786-0188 Post-Implementation Contact(s): Kimberly Downin kdownin@cms.hhs.gov 410-786-0188	**These instructions shall be implemented within your current operating budget.**

4.2.2 - Program Safeguard Contractor and Medicare Contractor Benefit Integrity Unit

(Rev.83 Issued:08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

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

- Prevents fraud by identifying program vulnerabilities.
- Proactively identifies incidents of fraud that exist within its service area and takes appropriate action on each case.
- Investigates (determines the factual basis of) allegations of fraud made by beneficiaries, providers, CMS, OIG, and other sources.
- Explores all available sources of fraud leads in its jurisdiction, including the MFCU and its corporate anti-fraud unit.
- Initiates appropriate administrative actions to deny or to suspend payments that should not be made to providers where there is reliable evidence of fraud.
- Refers cases to the Office of the Inspector General/Office of Investigations (OIG/OI) for consideration of civil and criminal prosecution and/or application of administrative sanctions (see PIM Chapter 4, §4.18ff, §4.19ff, and §4.20ff).
- Provides outreach to providers and beneficiaries.
- Initiates and maintains networking and outreach activities to ensure effective interaction and exchange of information with internal components as well as outside groups.

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

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

PSCs and Medicare contractor BI units shall take prompt action after scrutinizing billing practices, patterns, or trends that may indicate fraudulent billing, i.e., reviewing data for

inexplicable aberrancies (other than the expected) and relating the aberrancies to specific providers, identifying “hit and run” providers, etc. PSCs and Medicare contractor BI units shall meet periodically with staff from their respective internal components and PSCs shall also meet with AC staff to discuss any problems identified that may be a sign of potential fraud.

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

4.2.2.6 – Benefit Integrity Security Requirements

(Rev.83 Issued:08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

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, Medicare contractor BI unit, or MFIS, 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.

- MFISs. Typically, CMS would not expect MFISs to have routine access to fraud information. However, the MFISs may be directed by CMS to disseminate or convey certain privileged information. MFISs shall keep all sensitive information confidential.

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's 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.

4.3 – Medical Review for Benefit Integrity Purposes

(Rev.83 Issued:08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

The responsibilities of the PSCs and Medicare contractor BI units include looking for potential fraud. The MR unit's responsibilities include looking for potential errors. PSCs and Medicare contractor BI and MR staff shall work closely together, especially in the areas of:

- Data analysis *(PSCs shall follow Chapter 2, §2.3 for sources of data); and*
- Identification of potential errors or potential fraud (which shall be referred to the other component).

The PSCs, Medicare contractor BI units, and MR units shall have ongoing discussions and close working relationships regarding situations identified that may be signs of fraud. Intermediaries shall also include the cost report audit unit in the ongoing discussions.

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

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

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

PSCs and Medicare contractor BI units are also responsible for preventing and minimizing the opportunity for fraud. The PSCs and Medicare contractor BI units shall identify procedures that may make Medicare vulnerable to potential fraud and take appropriate action. For example, PSCs and Medicare contractor BI units may determine that there are problems in the provider enrollment process that make it possible for individuals excluded from the Medicare program to obtain a provider identification number. The PSCs and Medicare contractor BI units shall bring these vulnerabilities to the attention of the AC or Medicare contractor provider enrollment unit.

There may be situations where the PSC and Medicare contractor BI unit initiates the referral of potential fraud to the MR unit for a prepayment or postpayment medical determination. For example, the Medicare contractor BI unit may request the MR unit review claims and corresponding records associated with an investigation to determine if the services were performed at the level billed. The MR unit shall then return the investigation with their determination to the Medicare contractor BI unit.

Therefore, when the MR unit is requested by the Medicare contractor BI unit to perform medical review as part of an investigation, the MR costs shall be charged to the BI line (Activity Code 23007 in the BPR).

The PSC shall work with its own nurses to perform these types of reviews.

4.4.1 - Requests for Information from Outside Organizations

(Rev.83 Issued:08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

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's 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's 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. 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.

4.7.1 – Conducting Investigations

(Rev.83 Issued:08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

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

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

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

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

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

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

- Perform random validation checks of physician licensure.

- Review original CMNs.

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

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

- Initiate other analysis enhancements to authenticate proper payments.

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

Using internal data, PSCs and Medicare contractor BI units may determine the following:

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

- Type of services involved in the allegation.

- Places of service.

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

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

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

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

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

The purpose of these activities is to decide whether it is reasonable to spend additional investigative resources. If there appears to be a pattern, the PSC and Medicare contractor BI unit shall discuss it with OIG/OI at the onset of the investigation. The PSC and

Medicare contractor BI unit shall discuss with OIG/OI the facts of the investigation and obtain OIG's recommendation on whether or not the investigation should be further developed for possible case referral to OIG/OI.

Once a case has been referred to law enforcement, the PSC and Medicare contractor BI unit shall not contact the provider or their office personnel. If there is belief that provider contact is necessary, the PSC and Medicare contractor BI unit shall consult with OIG/OI. OIG/OI will consider the situation and, if warranted, concur with such contact. Additionally, if the suspect provider hears that its billings are being reviewed or learns of the complaint and contacts the PSC or the Medicare contractor BI unit, they shall report such contact immediately to OIG/OI.

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

4.8 - Disposition of Cases

(Rev.83 Issued:08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

A case exists when the PSC or Medicare contractor BI unit has referred a fraud allegation to law enforcement, including but not limited to documented allegations that: a provider, beneficiary, supplier, or other subject a) engaged in a pattern of improper billing, b) submitted improper claims with actual knowledge of their truth or falsity, or c) submitted improper claims with reckless disregard or deliberate ignorance of their truth or falsity. This definition of a case includes any and all allegations (regardless of dollar threshold or subject matter) where PSC or Medicare contractor BI unit staff verify to their own satisfaction that there is potential Medicare fraud (the allegation is likely to be true) and a referral to law enforcement has been performed. PSCs and Medicare contractor BI units do not prove fraud; such action is within the purview of the Department of Justice. Immediate advisements shall not be considered cases (see PIM Chapter 4, §4.18.1.2).

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

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

Once the case has been referred to OIG/OI, inform the complainant within 7 calendar days that the case has been referred to OIG/OI, and that further requests concerning the matter should be referred to OIG/OI. However, some cases may be sensitive and the

complainant is not to be informed of the referral to OIG/OI. The PSC and Medicare contractor BI unit shall contact OIG/OI before responding to the complainant if the case is a sensitive one. Otherwise, provide the complainant with the address of OIG/OI and the name of a contact person.

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

4.10.1 - Types of Fraud Alerts

(Rev.83 Issued:08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

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. The MFISs 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, All Medicare Carrier and Fiscal Intermediary 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 MFISs and/or PSCs. However, if the MFISs 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 MFIS one copy of an RMFA along with a sanitized version. Each MFIS 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 Carrier and Fiscal Intermediary 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.**

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 - Medicare Fraud Information Specialist or Program Safeguard Contractor 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 MFIS or PSC of the Alert denial.

- If the MFIS or PSC does not provide CMS with any additional information to justify reconsideration, the denial is final. However, the MFIS/PSC communication network may issue denied Alerts as MFIS/PSC Alerts.

- The MFIS and PSC shall provide the CMS CO Fraud Alert Lead with a copy of this Alert.

4.11.1 - Background

(Rev.83 Issued:08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

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, MFIS/PSC Network members, Medicaid Program Integrity Directors and Medicaid Fraud Control Units, and law enforcement agencies.

4.11.2 – Investigation, Case, and Suspension Entries

(Rev.83 Issued:08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

It is not appropriate for an OIG or FBI agent, DOJ, or an Assistant United States Attorney (AUSA), to request that a PSC or Medicare contractor BI unit not enter or update an investigation, case, or payment suspension initiated by the PSC or Medicare contractor BI unit in the FID, except in rare circumstances. PSCs and Medicare contractor BI units shall inform law enforcement agents making such requests that they are required by CMS to maintain the FID and that they do not have the discretion to do otherwise. The PSC or Medicare contractor BI unit shall contact the GTL, Co-GTL, and SME (if a PSC) or CMS RO employee (if a Medicare contractor BI unit) in order to resolve the matter.

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

4.11.2.1 - Initial Entry Requirements for Investigations

(Rev.83 Issued:08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

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.

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.

4.11.2.8 – Closing Investigations

(Rev.83, Issued: 08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

Investigations shall be closed when they are no longer reported as an investigation on the PSCs' ART or the Medicare contractor BI unit has determined that it will not result in a case (refer to §4.7.2 for a definition of when to close an investigation). The investigation that does not result in referral of a case shall be closed by entering the following action in the ACTIONS Tab in order to indicate that the investigation has been closed:

ACTIONS Tab:

- Action Taken by: Contractor

- Action: Investigation Closed

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

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

(Rev.83, Issued: 08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

PSCs and Medicare contractor BI units shall identify cases of suspected fraud and to 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.

Within 60 calendar days of identifying the necessity for administrative action (e.g., payment suspension or recoupment of an overpayment), the PSC and Medicare contractor BI unit shall consult with law enforcement prior to taking administrative action. 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 consult the GTL, Co-GTL, and SME and the Medicare contractor BI unit shall contact the RO. The GTL, Co-GTL, and SME for a PSC and the RO for a Medicare contractor BI unit will decide whether or not to take administrative action.

If 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 refer the case to the FBI and/or 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 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.

4.18.1.3.1 - Suspension

(Rev.83, Issued: 08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

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

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

PSCs and Medicare contractor BI units shall refer to PIM, Chapter 3, §3.9ff for suspension of payment instructions.

A - Record of Suspended Payments Regarding Providers Involved in Litigation

PSCs or Medicare contractor BI units shall provide OIG/OI with current information, as requested, regarding total payments due providers on monies that are being withheld because those cases are being referred for fraud prosecution. (The OIG/OI sends notification of which potential fraud cases have been referred for prosecution.) These monies represent potential assets, against which offset is made to settle overpayments or to satisfy penalties in any civil action brought by the government. The total amount of withheld payments is also pertinent to any determination by the DOJ whether civil fraud prosecution action is pursued or a negotiated settlement attempted.

4.18.3 - Referral to Quality Improvement Organizations

(Rev.83, Issued: 08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

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

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

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

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

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

The PSC shall coordinate the review of Part A acute care inpatient hospital claims *and long term care hospital PPS claims (i.e., long term acute care, not SNFs)* for benefit integrity purposes with the QIO. The PSC shall follow the definition of acute care inpatient prospective payment system (PPS) hospital found in PIM Chapter 1, §1.1.2

(http://www.cms.gov/manuals/108_pim/pim83c01.pdf). If the PSC investigation indicates a need to review Part A acute care inpatient PPS hospital medical records *or long term care hospital PPS claim medical records*, the PSC shall request the medical records directly from the provider and have them sent directly to the PSC. Upon receipt of the records, the PSC shall perform a billing and document review of the medical record. The PSC shall also review the medical records for medical necessity, as well as, any indications of potential fraud and abuse. The PSC shall not initiate any payment determination, provider education, overpayment calculation, or overpayment request based on these medical records. QIOs will conduct or initiate these activities as appropriate.

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

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

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

4.26.2 – Exceptions

(Rev.83, Issued: 08-27-04, Effective: September 27, 2004, Implementation: September 27, 2004)

Exceptions to the preceding statements concerning the date(s) of service on the claim occur when the items are provided in anticipation of discharge from a hospital or nursing facility. A supplier may deliver a DMEPOS item to a patient in a hospital or nursing facility for the purpose of fitting or training the patient in the proper use of the item. This may be done up to 2 days prior to the patient's anticipated discharge to their home. The supplier shall bill the date of service on the claim as the date of discharge and shall use the Place of Service (POS) as 12 (Patient's Home). The item must be for subsequent use in the patient's home. No billing may be made for the item on those days the patient was receiving training or fitting in the hospital or nursing facility.

A supplier may not bill for drugs or other DMEPOS items used by the patient prior to the patient's discharge from the hospital or a Medicare Part A nursing facility stay. Billing the DMERC for surgical dressings, urological supplies, or ostomy supplies that are provided in the hospital or during a Medicare Part A nursing facility stay is not allowed. These items are payable to the facility under Part A of Medicare. This prohibition applies even if the item is worn home by the patient from the hospital or nursing facility. Any attempt by the supplier and/or facility to substitute an item that is payable to the supplier for an item that, under statute, should be provided by the facility, may be considered to be fraudulent. These statements apply to durable medical equipment delivered to a patient in hospitals, skilled nursing facilities (Place of Service = 31), or nursing facilities providing skilled services (Place of Service = 32).

A supplier may deliver a DMEPOS item to a patient's home in anticipation of a discharge from a hospital or nursing facility. The supplier may arrange for actual delivery of the item approximately 2 days prior to the patient's anticipated discharge to their home. The supplier shall bill the date of service on the claim as the date of discharge and *shall* use the Place of Service (POS) as 12 (Patient's Home).