CMS Manual System

Pub. 100-08 Medicare Program Integrity

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

Transmittal 99 **Date: JANUARY 21, 2005**

CHANGE REQUEST 3646

SUBJECT: Program Integrity Manual Modification – Changes Waivers Approved by the Regional Office (RO) by Replacing Regional Office with Central Office (CO)

I. SUMMARY OF CHANGES: The Program Integrity Manual is being updated to provide instructions to contractors regarding waiver and exception requests that were submitted to the regional office for approval. This instruction changes the current language in the PIM from "waivers are approved by the RO" by replacing RO with CO.

NEW/REVISED MATERIAL - EFFECTIVE DATE*: March 24, 2004
IMPLEMENTATION DATE: February 22, 2005

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

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

R/N/D	CHAPTER/SECTION/SUBSECTION/TITLE
R	1/1.5/Contractor Medical Director (CMD)
R	4/4.2.2.6/Benefit Integrity Security Requirements
R	13/13.8.1/The Carrier Advisory Commitee

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

IV. ATTACHMENTS:

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

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

Attachment - Business Requirements

Pub. 100-08	Transmittal: 99	Date: January 21, 2005	Change Request 3646

SUBJECT: Program Integrity Manual Modification – Changes Waivers Approved by the Regional Office (RO) by Replacing Regional Office with Central Office (CO)

I. GENERAL INFORMATION

A. Background: Currently, the Program Integrity Manual (PIM) instructs contractors in Chapters: 1.5 – Contractor Medical Director; 4.2.2.6, A – Benefit Integrity Security Requirements; and 13.8.1 – The Carrier Advisory Committee that waivers are approved by the RO. This instruction modifies every instance in the PIM that says "waivers are approved by the RO" and replaces the RO reference with CO.

B. Policy: The Program Integrity Manual is being updated to provide instruction to contractors regarding waiver and exception requests that were submitted to the regional office for approval. This instruction changes the current language in the PIM from "waivers are approved by the RO" by replacing RO with CO.

C. Provider Education: None.

II. BUSINESS REQUIREMENTS

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

Requirement Number	Requirements	Responsibility ("X" indicates the columns that apply)								
		FI	RHHI	Carrier	DMERC	Shared System Maintainers				Other
						FISS	MCS	VMS	CWF	
3646.1	Contractors shall have their waivers for Program Safeguard and Medicare contractor operations approved by the CMS Central Office.	X	X	X	X					

III. SUPPORTING INFORMATION AND POSSIBLE DESIGN CONSIDERATIONS

A. Other Instructions: N/A

X-Ref Requirement #	Instructions

B. Design Considerations: N/A

X-Ref Requirement #	Recommendation for Medicare System Requirements

C. Interfaces: N/A

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

E. Dependencies: N/A

F. Testing Considerations: N/A

IV. SCHEDULE, CONTACTS, AND FUNDING

Effective Date*: March 24, 2004 **Implementation Date:** February 22, 2005 **Pre-Implementation Contact(s):** Sandra Latimer (410) 786-9178 **Post-Implementation Contact(s):** Sandra Latimer (410) 786-9178	**Medicare contractors shall implement these instructions within their current operating budgets.**

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

1.5 - Contractor Medical Director (CMD)

(Rev. 99, Issued: 01-21-05, Effective: 03-24-04, Implementation: 02-22-05)

Contractors must employ a minimum of one FTE contractor medical director and arrange for an alternate when the CMD is unavailable for extended periods. Waivers for very small contractors may be approved by the *CO*. The CMD FTE must be composed of no more than two physicians. All physicians employed or retained as consultants must be currently licensed to practice medicine in the United States, and the contractor must periodically verify that the license is current. When recruiting CMDs, contractors must give preference to physicians who have patient care experience and are actively involved in the practice of medicine. The CMD's duties are listed below.

Primary duties include:

- Leadership in the provider community, including:
    - Interacting with medical societies and peer groups;
    - Educating providers, individually or as a group, regarding identified problems or LMRP; and
    - Acting as co-chair of the Carrier Advisory Committee (CAC) (see PIM Chapter 13 §13.7.1.4 for co-chair responsibilities).
- Providing the clinical expertise and judgment to develop LMRPs and internal MR guidelines:
    - Serving as a readily available source of medical information to provide guidance in questionable claims review situations;
    - Determining when LMRP is needed or must be revised to address program abuse;
    - Assuring that LMRP and associated internal guidelines are appropriate;
    - Briefing and directing personnel on the correct application of policy during claim adjudication, including through written internal claim review guidelines;
    - Selecting consultants licensed in the pertinent fields of medicine for expert input into the development of LMRP and internal guidelines;
    - Keeping abreast of medical practice and technology changes that may result in improper billing or program abuse;
    - Providing the clinical expertise and judgment to effectively focus MR on areas of potential fraud and abuse; and
    - Serving as a readily available source of medical information to provide guidance in questionable situations.

Other duties include:

- Interacting with the CMDs at other contractors to share information on potential problem areas;
- Participating in CMD clinical workgroups, as appropriate; and
- Upon request, providing input to CO on national coverage and payment policy, including recommendations for relative value unit (RVU) assignments.

To prevent conflict of interest issues, the CMD must provide written notification to CO (MROperations@cms.hhs.gov) and RO (for PSCs, the GTL, Co-GTL, and SME), as well as to the CAC, within 3 months after the appointment, election, or membership effective date if the CMD becomes a committee member or is appointed or elected as an officer in any State or national medical societies or other professional organizations. In addition, CMDs who are currently in practice should notify their RO (for PSCs, the GTL, Co-GTL, and SME) of the type and extent of the practice.

4.2.2.6 – Benefit Integrity Security Requirements

(Rev. 99, Issued: 01-21-05, Effective: 03-24-04, Implementation: 02-22-05)

The PSCs and Medicare contractors shall ensure a high level of security for this sensitive function. PSCs and Medicare contractor BI unit staff, as well as all other PSC and Medicare contractor employees, shall be adequately informed and trained so that information obtained by, and stored in, the PSC and Medicare contractor BI unit is kept confidential.

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

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

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

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

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

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

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

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

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

- Barring budget constraints and a specific written waiver (exception) from the CMS *RO*, the Medicare contractor BI unit shall be completely segregated from all other Medicare contractor operations. This segregation shall include closed walls or partitions that prevent unauthorized access or overhearing of sensitive investigative information. Full PSCs are not required to separate their MR and BI units. However, all BI information shall be kept confidential and secure and shared with MR only on a need-to-know basis.

B - Handling and Physical Security of Sensitive Material

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

The following guidelines shall be followed:

- Employees shall discuss specific allegations of fraud only within the context of their professional duties and only with those who have a valid need to know. This may include staff from the PSC, AC or Medicare contractor MR or audit units, data analysis, senior management, or corporate counsel.

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

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

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

- For mail processing sites located in separate PSC or Medicare contractor facilities, the PSC or Medicare contractor shall minimize the handling of BI unit

mail by multiple parties before delivery to the PSC or Medicare contractor BI unit.

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

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

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

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

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

C - Designation of a Security Officer

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

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

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

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

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

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

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

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

D - Staffing of the Program Safeguard Contractor or Medicare Contractor Benefit

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

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

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

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

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

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

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

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

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

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

E - Access to Information

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

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

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

- Corporate employees working outside the Medicare division.

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

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

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

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

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

F - Computer Security

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

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

- Access to computer files containing information on current or past fraud investigations shall be given only to employees who need such access to perform their official duties.
- Passwords permitting access to BI compatible files or databases shall be kept at the level of confidentiality specified by the PSC or Medicare contractor BI unit supervisory staff. Employees entering their passwords shall ensure that it is done at a time and in a manner that prevents unauthorized persons from learning them.

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

- Another safe and efficient way to preserve data is to back it up. Backing up data is similar to copying it, except that back-up utilities compress the data so that less disk space is needed to store the files.
- Record sensitive information on specially marked floppy disks or CDs and control and file these in a secure container placed in a locked receptacle (desk drawer, file cabinet, etc.). Check computers used for sensitive correspondence to ensure that personnel are not filing or backing up files on the hard drive. The configuration of the software needs to be checked before and after the computer is used to record sensitive information.

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

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

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

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

Environmental security measures shall also be taken as follows:

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

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

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

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

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

G - Telephone Security

The PSC or Medicare contractor BI unit shall implement phone security practices. As stated earlier in this section, the PSC or Medicare contractor BI unit shall discuss investigations and cases only with those individuals that have a need to know the information, and shall not divulge information to individuals not personally known to the PSC or Medicare contractor BI unit involved in the investigation of the related issue. This applies to persons unknown to the PSC or Medicare contractor BI unit who say they are with the FBI, OIG, DOJ, etc. The PSC or Medicare contractor BI unit shall only use CMS, OIG, DOJ, and FBI phone numbers that can be verified. Management shall provide PSC or Medicare contractor BI unit staff with a list of the names and telephone numbers of the individuals of the authorized agencies that the PSC or Medicare contractor BI unit deal with and shall ensure that this list is properly maintained and periodically updated.

Employees shall be polite and brief in responding to phone calls, but shall not volunteer any information or confirm or deny that an investigation is in process. Personnel shall be cautious of callers who “demand” information and continue to question the P SC 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.

13.8.1 - The Carrier Advisory Committee

(Rev. 99, Issued: 01-21-05, Effective: 03-24-04, Implementation: 02-22-05)

Carriers shall establish one CAC per State. Where there is more than one carrier in a State, the carriers shall jointly establish a CAC. If there is one carrier for many States, each State shall have a full committee and the opportunity to discuss draft LCDs and issues presented in their State. Carriers maintain a current directory of CAC members which is available to CO, RO *(for PSCs, the GTL, Co-GTL, and SME)* staff, and the provider community on request. Carriers that develop identical policies for their entire jurisdiction may establish a single CAC *if they are granted a waiver* from the CO *(for PSCs, the GTL, Co-GTL, and SME)*. In order to obtain a waiver from the *CO (for PSCs, the GTL, Co-GTL, and SME)*, contractors shall obtain agreement from CAC members within the jurisdiction.