Medicare Program Integrity Manual

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

Transmittal 19 **Date: FEBRUARY 8, 2002**

CHANGE REQUEST 1907

CHAPTERS	REVISED SECTIONS	NEW SECTIONS	DELETED SECTIONS
1	3.2.6		

NEW/REVISED MATERIAL--EFFECTIVE DATE: February 8, 2002
IMPLEMENTATION DATE: February 8, 2002

Chapter 1, Section 3.2.6, Security Requirements -- clarifies all Benefit Integrity Unit security requirements.

These instructions should be implemented within your current operating budget.

NOTE: Red italicized font identifies new material.

3.2.6 – Security Requirements - (Rev. 19, 02-08-02)

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

Physical and operational security within the *BI* unit is essential. Operational security weaknesses in the *BI* unit's day to day activities may be less obvious and more difficult to identify and correct than physical security. The *BI* unit's interaction with other 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" located on www.hcfa.gov/extpart, and it is being reemphasized in this PIM section.

A – Privacy of *Benefit Integrity* Unit Operations

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

- Limiting access to *BI* unit sites to only those who need to be there on official business (Tours of the 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 *BI* unit who are there for official purposes, unrelated to *BI* unit functions (e.g., cleaning crews, mail delivery personnel, technical equipment repair staff) are not left unobserved;
- Securing the *BI* unit site when it is not occupied by *BI* unit personnel; and
- *Barring budget constraints and a specific written waiver (exception) from the CMS RO, the contractor BI unit shall be completely segregated from all other contractor operations. This segregation shall include closed walls or partitions that prevent unauthorized access or overhearing of sensitive investigative information.*

B – Handling and Physical Security of Sensitive Material

Consider all fraud and abuse allegations and associated case development material to be sensitive material. The term "sensitive material" includes, but is not limited to, *BI* unit 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, *and potentially jeopardize the personal safety of law enforcement (e.g., covert/undercover investigations).*

The following guidelines *shall* be followed:

- Employees *shall* only discuss specific allegations of fraud within the context of their professional duties and only with those who have a valid need to know. This may include staff from the MR or audit units, 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 and provides assurance that mail contents will not be read and will be held in confidence.* Mail being sent to CO, another *BI* unit, or MFIS, should 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 contractor facilities, the contractor shall minimize the handling of BIU mail by multiple parties before delivery to the BIU;*

- 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*;

- Contractors *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 contractors *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 unit *shall* maintain a "controlled" filing system. (see PIM Chapter 1, §3.2.4.1); and

- *Discarded sensitive information shall be immediately shredded or stored in a locked container for subsequent shredding.*

C – Designation of a Security Officer

The *BI* unit manager *shall* designate an employee to serve as the security officer of the 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 below 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; and

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

The *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; and

- 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 BI unit manager.*

D – Staffing of the *Benefit Integrity* Unit and Security Training

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

When hiring BI unit employees, the individual should have easily verifiable character references and a record of stable employment.

The *BI* unit manager *shall* ensure the following:

- Thorough background and character reference checks *shall* be performed for

potential employees to verify *their* suitability for employment with the *BI* unit;

- In addition to conducting a thorough background investigation, potential employees *shall* be asked whether their employment in the *BI* unit might involve a conflict of interest;

- 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, students (non-paid or interns) and non-citizens shall not be employed in the BI unit;

- *At the point a hiring decision is made for a BI 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;*

- The special security considerations under which the *BI* unit operates *shall* be thoroughly explained and discussed; and

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

E – Access to Information

Contractor and *CMS* managers, *shall* have routine access to sensitive information if the contractors and *CMS* managers are specifically authorized to work directly on a particular fraud case or are reviewing cases as part of a CPE review. 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 includes the following:

- employees who are not part of the Medicare contractor;

- corporate employees working outside the Medicare division;

- clerical employees *who are not integral part of the BI unit*; and

- 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 should 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*, contractors *shall not* release information to any person *outside of the 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," contractors have no legal obligation to comply with such requests. The contractors *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, contractors *shall* definitely determine that a caller has a "need to know," and that furnishing the requested information will not prejudice the case or prove harmful in any other way. *Each case file shall list the name, organization, address and telephone numbers of all persons with whom the contractor can discuss the case (including those working within the BI unit).*

While contractor management may have access to general case information, it *shall only request on a need to know basis* specific information about cases that the *BI* unit is actively developing.

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

F – Computer Security

Access to computers *shall* be granted only to *BI* unit employees. The following guidelines *shall* be followed:

- *Comply with all parameters/standards in CMS's "Information System Security Policy, Standards and Guidelines Handbook" and "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 contractor* 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;

- *Unless the following two exceptions are met,* computer files with sensitive information *shall* never be filed or backed up on the hard drive of personal computers*: 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; *2) the computer can be protected (secured with a "boot" password. The "boot password" is a password that is entered after the computer is turned on (powered on). This password prevents unauthorized users from accessing any information stored on the computer's local hard drive(s) (C drive, D drive). Unless one of the two exceptions have been met,* the only files to be stored permanently on the computer hard drive are applications software;

- Permanent storage on a floppy disk *or compatible disk (CD)* is a safe and

efficient way to preserve data and enhances security, since the disks can be locked up. The concept is to write directly to a floppy disk *or CD*. An option is to use the hard drive for storage until the product is completed, then transfer the file to a floppy disk for permanent storage and delete it from the hard 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 must be located on a secure Server and the LAN/WAN drive must 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 that designated for the BI unit. As such, LAN/WAN Administrators must 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, 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*; and

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

G – Telephone Security

The *BI* unit *shall* implement phone security practices. *As stated earlier in this section, the BI unit* discusses cases only with those individuals that have a **need to know** the information and never divulge information to individuals not personally known to the contractor *or involved in the investigation of the related issue.*

This applies to persons unknown to the contractor who say they are with the FBI, OIG, DOJ, etc. Only use *CMS*, OIG, DOJ, and FBI phone numbers that can be verified. Management *shall* provide *BI* unit staff with a list of the names and telephone numbers of the individuals of the authorized agencies that the contractor deals with and ensures that this list is properly maintained and periodically updated.

Employees are polite and brief in responding to phone calls, but do not volunteer any information or confirm or deny that an investigation is in process. Personnel are especially cautious of callers who "demand" information and continue to question the contractor 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. Contractors do not respond to questions concerning any case being investigated by the OIG, FBI*, or any other law enforcement agency.* The contractors refer them to the OIG, FBI, *etc.* as appropriate.

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,* contractors *shall* make arrangements with the addressee to have someone waiting at the receiving machine while the FAX is being transmitted. Never transmit sensitive information via FAX when it is necessary to use a delay feature such as entering the information into the machine's "memory".