CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-08 Medicare Program Integrity	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 675	**Date: September 9, 2016**
	Change Request 9426

SUBJECT: Update to Chapter 4, Pub. 100-08

I. SUMMARY OF CHANGES: The purpose of this change request (CR) is to revise certain program integrity investigation instructions in chapter 4 of Pub. 100-08.

EFFECTIVE DATE: December 12, 2016
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION December 12, 2016

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

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

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
R	4/Table of Contents/Program Integrity
R	4/4.1/Introduction
R	4/4.1.1/Definitions
R	4/4.2/The Medicare Fraud Program
R	4/4.2.1/Examples of Medicare Fraud
R	4/4.2.2/Zone Program Integrity Contractor
R	4/4.2.2.1/Organizational Requirements
R	4/4.2.2.2/Liability of Zone Program Integrity Contractor Employees
R	4/4.2.2.3/Anti-Fraud Training
R	4/4.2.2.3.1/Training for Law Enforcement Organizations
R	4/4.2.2.4/Procedural Requirements
R	4/4.2.2.4.1/Maintain Controlled Filing System and Documentation
R	4/4.2.2.6/Program Integrity Security Requirements
R	4/4.3/Medical Review for Program Integrity Purposes
R	4/4.4.1/Requests for Information From Outside Organizations
R	4/4.4.1.1/Reserved for Future Use
R	4/4.4.2/Zone Program Integrity Contractor Coordination With Other Zone Program Integrity Contractors
R	4/4.4.2.1/Zone Program Integrity Contractor Coordination With Other Entities
R	4/4.4.3/Reserved for Future Use
R	4/4.5/Reserved for Future Use
R	4/4.6.1/Definition of a Complaint
R	4/4.6.2/Complaint Screening
N	4/4.6.2.1/Zone Program Integrity Contractor Responsibilities
R	4/4.6.3/Screening Leads
N	4/4.6.4/Vetting Leads with CMS
R	4/4.7/Investigations
R	4/4.7.1/Conducting Investigations

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
R	4/4.7.2/Closing Investigations
N	Exhibit 47/ Program Integrity Unit Contacts within the State Medicaid Agency

III. FUNDING:

For Medicare Administrative Contractors (MACs):

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

IV. ATTACHMENTS:

Business Requirements
Manual Instruction

Attachment - Business Requirements

Pub. 100-08	Transmittal: 675	Date: September 9, 2016	Change Request: 9426

SUBJECT: Update to Chapter 4, Pub. 100-08

EFFECTIVE DATE: December 12, 2016
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: December 12, 2016

I. GENERAL INFORMATION

A. Background: Chapter 4 of Pub. 100-08 contains instructions regarding the performance of program integrity (PI) investigations. This CR revises and clarifies certain policies involving PI investigations. These changes are intended to streamline existing procedures.

B. Policy: This CR does not involve any legislative or regulatory policies.

II. BUSINESS REQUIREMENTS TABLE

"Shall" denotes a mandatory requirement, and "should" denotes an optional requirement.

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
9426.1	When the Zone Program Integrity Contractor (ZPIC) makes the determination of potential fraud, waste, or abuse, the ZPIC shall effectuate all appropriate administrative actions and refer the case to the Office of Inspector General (OIG), if appropriate.									ZPICs
9426.2	The ZPIC shall prioritize the top 100 Alert Summary Records (ASRs) in the Fraud Prevention System (FPS) along with other investigation work based on the prioritization									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	requirements outlined in section 4.2.2.1 of chapter 4.									
9426.3	The ZPIC shall hire and retain employees who are qualified to testify in a criminal and civil trial when requested by law enforcement.									ZPICs
9426.4	The ZPIC shall notify via e-mail the Contracting Officer's Representative (COR) and the Centers for Medicare & Medicaid Services' (CMS) Investigations & Audits Group (IAG) Business Function Lead (BFL) when the ZPIC is asked to accompany the OIG/Office of Investigations (OI) or any other law enforcement agency onsite to a provider/supplier for the purpose of gathering evidence in potential fraud case.									ZPICs
9426.4.1	As stated in section 4.2.2.4 of chapter 4, the ZPIC personnel shall (1) properly identify themselves as ZPIC employees, (2) under no circumstances represent themselves as law enforcement personnel or special agents, and (3) under no circumstances accompany law enforcement in situations where their personal safety									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	is in question.									
9426.5	The ZPIC shall assist in preparing and developing fraud-related articles for Medicare Administrative Contractor (MAC) newsletters/bulletins; once completed, the ZPIC shall submit such materials to the following e-mail address: CPIFraudRelatedLeads@cms.hhs.gov, with a copy to the CORs and IAG BFLs.									ZPICs
9426.6	The MAC shall implement parameters for the edits/audits described in section 4.3(B) of chapter 4 within the timeframe established in the MAC and ZPIC Joint Operating Agreement (JOA), which shall not exceed more than 15 business days.	X	X	X	X					
9426.7	In carrying out section 4.3(C)(6) of chapter 4, the ZPIC shall not consider undated or unsigned entries handwritten in the margin of a document; these entries shall be excluded from consideration when performing medical review.									ZPICs
9426.8	The ZPIC shall establish a Quality Improvement (QI) process that verifies the accuracy of medical review decisions made by									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	licensed health care professionals; ZPICs shall include inter-rater reliability and/or peer-review assessments in their QI process and shall report these results as directed by CMS.									
9426.9	If the information request referred to in section 4.4.1(B) of chapter 4 concerns an investigation(s) already referred to the OIG/OI, the ZPIC shall notify the OIG/OI of the request for information received from another ZPIC and notify the requesting ZPIC that the case has been referred to the OIG/OI.									ZPICs
9426.10	With respect to requests from the OIG/OI for data and other records (as referenced in section 4.4.1(G)), the ZPIC shall not fulfill a request if there is a substantial impact (i.e., 40 hours or more) on the budget without prior COR approval.									ZPICs
9426.10.1	For Priority I requests, the ZPIC shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested within 30 calendar days or sooner, when possible.									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
9426.10.1.1	The MAC shall furnish requested information to the ZPIC within 20 calendar days of receipt of the request from the ZPIC unless there are extenuating circumstances.	X	X	X	X					
9426.10.1.2	The MAC shall communicate any extenuating circumstances to the ZPIC and the MAC COR as soon as they become known.	X	X	X	X					
9426.10.1.3	The ZPIC shall communicate the extenuating circumstances referred to in business requirement 9426.10.1.2 to its COR.									ZPICs
9426.10.1.4	If extenuating circumstances exist that prevent the ZPIC from meeting the 30-day timeframe, the ZPIC shall inform the requestor what, if any, portion of the request can be provided within 30 calendar days.									ZPICs
9426.10.2	For the Priority II requests described in section 4.4.1(G) of chapter 4, the MAC shall furnish requested information to the ZPIC within 30 calendar days of receipt of the request from the ZPIC unless there are extenuating circumstances; the MAC shall communicate any	X	X	X	X					ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	extenuating circumstances to the ZPIC and the MAC COR as soon as they become known, and the ZPIC shall communicate these extenuating circumstances to its COR.									
9426.10.2.1	If extenuating circumstances exist that prevent the ZPIC from meeting the applicable 45-day timeframe, the ZPIC shall inform the requestor what, if any, portion of the request can be provided within 45 calendar days.									ZPICs
9426.11	When the OIG makes a data request, the ZPIC shall track these requests and document the following: (1) nature/purpose of the disclosure; (2) what information was disclosed; and (3) name of the individual and the agency. (The aforementioned information shall be maintained in a secure file and made available to CMS upon request through a secure means.)									ZPICs
9426.11.1	If the estimated level of effort to fulfill any one request is likely to meet or exceed 40 hours, the ZPIC shall contact its COR for approval to proceed.									ZPICs
9426.11.2	The ZPIC shall obtain approval from the COR									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	regarding requests started by the ZPIC that it subsequently anticipates will exceed that 40-hour level of effort. (The ZPIC shall not exceed the 40-hour level of effort until it receives COR approval.)									
9426.12	For Department of Justice (DOJ) data requests labeled Priority I, the ZPIC shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested within 30 calendar days or sooner, when possible.									ZPICs
9426.12.1	The MAC shall furnish requested information to the ZPIC within 20 calendar days of receipt of the request from the ZPIC unless there are extenuating circumstances; the MAC shall communicate any extenuating circumstances to the ZPIC and the MAC COR as soon as they become known.	X	X	X	X					
9426.12.1.1	The ZPIC shall communicate these extenuating circumstances to its COR. (If extenuating circumstances exist that prevent the ZPIC from meeting the thirty (30) day timeframe, the ZPIC shall inform the requestor what, if any, portion of the request can be provided									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	within thirty (30) days.)									
9426.13	For DOJ data requests labeled Priority II, the ZPIC shall respond to such requests within 45 calendar days or sooner, when possible.									ZPICs
9426.13.1	The MAC shall furnish requested information to the ZPIC within 30 calendar days of receipt of the request from the ZPIC unless there are extenuating circumstances; the MAC shall communicate any extenuating circumstances to the ZPIC and the MAC COR as soon as they become known, and the ZPIC shall communicate these extenuating circumstances to its COR.	X	X	X	X					ZPICs
9426.13.1.1	If extenuating circumstances exist that prevent the ZPIC from meeting the applicable 45-day timeframe, the ZPIC shall inform the requestor what, if any, portion of the request can be provided within 45 calendar days.									ZPICs
9426.14	For law enforcement requests for assistance, the ZPIC shall negotiate due dates with the requesting entity and document appropriately, along with the reasons for not meeting the agreed upon									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	timeframes; the ZPIC shall contact the COR if an agreement cannot be reached on the timeframe for completion.									
9426.14.1	The ZPIC shall ensure that disclosures of information to the DOJ comply with the Privacy Rule and Privacy Act.									ZPICs
9426.14.2	When the DOJ makes a data request, the ZPIC shall track these requests and document the following: (1) nature/purpose of the disclosure, (2) what information was disclosed, and (3) name of the individual and the agency. (The aforementioned information shall be maintained in a secure file and made available to CMS upon request through a secure means.)									ZPICs
9426.14.3	If the estimated level of effort to fulfill any one request is likely to meet or exceed 40 hours, the ZPIC shall contact its COR for approval to proceed.									ZPICs
9426.14.3.1	The ZPIC shall obtain approval from the COR regarding requests started by the ZPIC that it subsequently anticipates will exceed the 40-hour level of effort; the ZPIC shall not exceed the 40-									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	hour level of effort until it receives COR approval.									
9426.14.4	If a ZPIC receives a request from law enforcement for information that crosses several ZPIC zones, the ZPIC shall contact its COR and IAG BFL.									ZPICs
9426.14.4.1	If multiple zones are providing information in connection with the request, each ZPIC shall enter a separate entry into the Fraud Investigation Database (FID) as described in section 4.11.2.8 of chapter 4.									ZPICs
9426.15	The ZPIC shall refer complaints alleging poor quality of care to the Medicare/Medicaid survey and certification agencies and the Quality Improvement Organizations (QIOs) within two (2) business days.									ZPICs
9426.15.1	The ZPIC shall forward any medical records to the QIO upon receipt from the provider, when appropriate.									ZPICs
9426.15.2	The ZPIC shall ensure that any complaints involving allegations of fraud are screened to determine if further investigation by the									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	ZPIC is necessary.									
9426.15.3	The MAC shall refer complaints alleging poor quality of care to the QIO.	X	X	X						
9426.16	For second-level screening as described in section 4.6.2(B) of chapter 4, the MAC shall perform a more in-depth review if additional complaints or inquiries are received; complaints or inquiries that do not meet the threshold for second-level screening shall be closed.	X	X	X	X					
9426.16.1	If the MAC staff determines that the complaint or inquiry is not a fraud and/or abuse issue and if the staff discovers that the complaint or inquiry has other issues (e.g., medical review, enrollment, claims processing), the MAC shall refer the complaint or inquiry to the appropriate department and then close it.	X	X	X	X					
9426.16.2	If the MAC requests additional documentation that is received after the 45-business day timeframe and the complaint is closed, the complaint shall be reopened but only if the additional information warrants further action or if the additional information would change	X	X	X	X					

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	the initial determination.									
9426.16.3	Once the complaint has been referred to the ZPIC, the MAC shall close the complaint in its internal tracking system.	X	X	X	X					
9426.16.4	To refer an erroneously assigned complaint to a MAC, the referring contractor shall send an e-mail containing all relevant complaint information and documents to the correct contractor notifying it that a complaint is being reassigned.	X	X	X	X					
9426.16.4.1	Within 10 business days of receiving the e-mail, the receiving contractor shall review the complaint.	X	X	X	X					
9426.16.5	The MAC shall refer complaints alleging fraud, waste, or abuse in the Medicaid program to the appropriate Program Integrity Unit (PIU) within the State Medicaid Agency (SMA) noted in Exhibit 47.	X	X	X	X					
9426.16.5.1	The MAC shall send the complaint information with any supporting documents to the appropriate PIU.	X	X	X	X					
9426.16.6	The MAC shall identify and refer complaints alleging fraud, waste, or	X	X	X	X					

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	abuse in the Medicare Part C or Part D programs to the Medicare Drug Integrity Contractor (MEDIC); this includes complaints that do not have a credible allegation of fraud.									
9426.16.7	If applicable under section 4.6.2(B) of chapter 4, the MAC shall refer complaints in accordance with said section.	X	X	X	X					
9426.16.8	When a provider/supplier inquiry or complaint of potential fraud or immediate advisement is received, the MAC's second-level screening staff shall not perform any screening but shall prepare a referral package within two business days of when this inquiry or immediate advisement was received, and send it to the ZPIC during the same timeframe.	X	X	X	X					
9426.17	When the complaint is received from the MAC screening staff, the ZPIC shall further screen the complaint, resolve the complaint, or make referrals as needed to the appropriate entity.									ZPICs
9426.17.1	The MAC shall screen and forward the complaints within 45 business days from the date of receipt by	X	X	X	X					

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	the second-level screening staff, or within 30 business days of receiving medical records and/or other documentation, whichever is later, to the ZPIC.									
9426.17.1.1	The ZPIC shall send the acknowledgement letter within 15 calendar days of receipt of the complaint referral from the MAC second-level screening staff, unless it can be resolved sooner; said letter shall be sent on ZPIC letterhead and shall contain the telephone number of the ZPIC analyst handling the case.									ZPICs
9426.17.1.2	If the ZPIC staff determines, after screening the complaint, that it is not a potential fraud, waste, and/or abuse issue, but involves other issues (e.g., medical review, enrollment, claims processing), the ZPIC shall refer the complaint to the MAC area responsible for second-level screening.									ZPICs
9426.17.1.3	The MAC second-level screening staff shall track the complaints returned by the ZPIC; however, the ZPIC shall send an acknowledgement to the complainant, indicating that a referral is being made, if applicable, to the appropriate MAC unit for	X	X	X	X					ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	further action.									
9426.17.2	The ZPIC shall track complaints referred by the MAC second-level screening area in the ZPIC's internal tracking system.									ZPICs
9426.17.3	The ZPIC shall send the complainant a resolution letter within seven (7) calendar days of resolving the complaint investigation.									ZPICs
9426.18	As stated in section 4.6.3 of chapter 4, the ZPIC shall complete screening within 21 calendar days after receipt of the lead.									ZPICs
9426.18.1	The ZPIC shall note that any screening activities shall not involve contact with the subject provider/supplier or implementation of any administrative actions (i.e., post-payment reviews, prepayment reviews/edits, payment suspensions, and revocations).									ZPICs
9426.18.2	If the lead involves potential patient harm, the ZPIC shall immediately notify CMS within two (2) business days.									ZPICs
9426.18.3	After completing its screening, the ZPIC shall close the lead if it does not									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	appear to be related to fraud, waste, or abuse; prior to closing the lead, the ZPIC shall take any appropriate actions.									
9426.18.4	At a minimum, the ZPIC shall document in its case file and the FID the information described in section 4.6.3 of chapter 4.									ZPICs
9426.18.5	If the screening process exceeds 21 calendar days, the ZPIC shall document the reasons, circumstances, dates, and actions associated with the delay to its COR and IAG BFL within its monthly reporting in the CMS Analysis, Reporting, and Tracking System.									ZPICs
9426.18.6	As all leads and any new subjects that the ZPIC determines warrant further investigation shall be vetted through CMS for approval before transitioning to an investigation, the ZPIC shall submit the lead to CMS within two (2) business days of the ZPIC determining that the lead should be transitioned into an investigation; for the submission to CMS, the ZPIC shall use the designated CMS Vetting Form, which shall include, at a minimum, National Provider Identifier (NPI),									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	name, and practice location.									
9426.18.7	The ZPIC shall only open investigations on leads that are approved by CMS.									ZPICs
9426.18.8	If the ZPIC is instructed by CMS to close the lead without further action, the ZPIC shall do so within two (2) business days.									ZPICs
9426.18.9	If, during the course of a ZPIC investigation, it is determined that additional NPIs should be incorporated into the ongoing investigation, the ZPIC shall vet each additional NPI with CMS utilizing the approved CMS process before implementing any investigative actions on the additional NPIs.									ZPICs
9426.18.10	For any new investigations, the ZPIC shall complete the appropriate updates in the FID within seven (7) calendar days.									ZPICs
9426.19	As stated in section 4.7 of chapter 4, the ZPIC shall focus its investigation in an effort to establish the facts and the magnitude of the alleged fraud, waste, or abuse and take any appropriate action to protect Medicare Trust									ZPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	Fund dollars.									
9426.19.1	For any investigative activities that require preapproval by CMS (i.e., payment suspensions, and revocations), the ZPIC shall submit those requests to CMS for approval with a copy to its COR and BFLs for approval when initiating those actions.									ZPICs
9426.20	If the ZPIC determines that an overpayment exists solely on data analysis, the ZPIC shall obtain COR and IAG BFL approval prior to initiating the overpayment.									ZPICs

III. PROVIDER EDUCATION TABLE

Number	Requirement	Responsibility				
		A/B MAC			DME MAC	CEDI
		A	B	HHH		
	None					

IV. SUPPORTING INFORMATION

Section A: Recommendations and supporting information associated with listed requirements:

"Should" denotes a recommendation.

X-Ref Requirement Number	Recommendations or other supporting information:

Section B: All other recommendations and supporting information: N/A

V. CONTACTS

Pre-Implementation Contact(s): Frank Whelan, 410-786-1302 or frank.whelan@cms.hhs.gov

Post-Implementation Contact(s): Contact your Contracting Officer's Representative (COR).

VI. FUNDING

Section A: For Medicare Administrative Contractors (MACs):
The Medicare Administrative Contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the MAC Statement of Work. The contractor is not obligated to incur costs in excess of the amounts allotted in your contract unless and until specifically authorized by the Contracting Officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the Contracting Officer, in writing or by e-mail, and request formal directions regarding continued performance requirements.

ATTACHMENTS: 0

Medicare Program Integrity Manual
Chapter 4 - *Program* Integrity

Table of Contents
(Rev.675, Issued: 09-09-16)

4.1 - Introduction

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

CMS Pub. 100-08, Program Integrity Manual (PIM)*,* reflects the principles, values, and priorities of the Medicare Integrity Program (MIP). The primary principle of *p*rogram *i*ntegrity (PI) is to pay claims correctly. *T*o meet this goal, *Zone Program Integrity Contractors (*ZPICs*)* and Medicare *Administrative C*ontractors (MACs) must ensure that *Medicare* pay*s* the right amount for covered and correctly coded services rendered to eligible beneficiaries by legitimate providers. The Centers for Medicare & Medicaid Services (CMS) follows four parallel strategies in meeting this goal:

1. *P*revent fraud through effective enrollment and education of providers*/suppliers* and beneficiaries*;*
2. *Encourage* early detection *(*through, for example, *the Fraud Prevention System (FPS),* medical review *(MR)* and data analysis*);*
3. *Coordinate* close*ly* with partners, including *other* ZPICs, MACs, law enforcement *(LE)* agencies*, and State Program Integrity units;* and
4. *Enact* fair and firm enforcement policies.

The ZPICs shall follow the PIM to the extent outlined in their respective task orders' *Statement of Work (SOW)*. The ZPICs shall only perform the functions outlined in the PIM as they pertain to their own operation. The ZPIC*s*, in partnership with CMS, shall be proactive and innovative in finding ways to enhance the performance of PIM guidelines.

For this entire chapter, and until such time as all ZPICs are awarded, any reference to ZPICs shall also apply to Program Safeguard Contractors (PSCs), unless otherwise noted. All references to ZPICs shall also apply to Unified Program Integrity Contractor (UPIC) unless otherwise specified in the UPIC SOW. MACs shall follow the PIM in accordance with their SOW.

4.1.1 - Definitions

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

To facilitate understanding, the terms used in the PIM are defined in PIM Exhibit 1. *The acronyms used in the PIM are listed in PIM Exhibit 23*.

4.2 - The Medicare Fraud Program

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs and MACs, as indicated.

The primary goal of the ZPIC is to identify cases of suspected fraud, waste and abuse, develop them thoroughly and in a timely manner, and take immediate action to ensure that Medicare Trust Fund monies are not inappropriately paid. *Payment* suspension and denial of payments and the recoupment of overpayments are example*s* of the actions that may be taken. *Once such actions are taken,* cases *where there is* potential fraud are referred to the OIG/Office of Investigations *(OI)* field office for consideration and initiation of criminal or civil prosecution, civil monetary penalt*ies*, or administrative sanction actions.

Preventing and detecting *fraud, waste, and abuse* involves a cooperative effort among beneficiaries*;* ZPICs*;* MACs*;* providers*/suppliers;* quality improvement organizations (QIOs)*;* s*tate* Medicaid fraud control units (MFCUs)*; state Medicaid Program Integrity units;* and federal agencies such as CMS*;* the Department of Health and Human Services (HHS)*; the* OIG*;* the Federal Bureau of Investigation (FBI)*;* and the Department of Justice (DOJ).

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

investigation. *When the ZPIC makes the determination of potential fraud, waste, or abuse, the ZPIC shall effectuate all appropriate administrative actions and refer the case to the OIG, if appropriate.* When the ZPIC *makes the determination* that a situation is not *potential* fraud, *the ZPIC* shall *close the matter, or* refer the situation to the appropriate unit at the MAC*, QIO, Recovery Auditor (RA), or other entity, when appropriate*.

4.2.1 - Examples of Medicare Fraud

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs and MACs.

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

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

Fraud may take such forms as *(this is not an exhaustive list)*:

- Incorrect reporting of diagnoses or procedures to maximize payments;
- Billing for services not furnished and/or supplies not provided. This includes billing Medicare for appointments that the patient failed to keep;
- Billing that appears to be a deliberate application for duplicate payment for the same services or supplies, billing both Medicare and the beneficiary for the same service, or billing both Medicare and another insurer in an attempt to get paid twice;
- Altering claim forms, electronic claim records, medical documentation, etc., to obtain a higher payment amount;
- Soliciting, offering, or receiving a kickback, bribe, or rebate *(*e.g., paying for a referral of patients in exchange for the ordering of diagnostic tests and other services or medical equipment*)*;
- Unbundling or “exploding” charges;
- Completing Certificates of Medical Necessity *f*or patients not personally and professionally known by the provider;
- Participating in schemes that involve collusion between a provider and a beneficiary, or between a supplier and a provider, *that* result in higher costs or charges to the Medicare program;
- Participating in schemes that involve collusion between a provider and a MAC employee where the claim is assigned *(*e.g., the provider deliberately overbills for services, and the MAC employee then generates adjustments with little or no awareness on the part of the beneficiary*)*;
- Billing based on “gang visits,” *(*e.g., a physician visits a nursing home and bills for 20 nursing home visits without furnishing any specific service to individual patients*)*;
- Misrepresent*ing* dates and descriptions of services furnished or the identity of the beneficiary or the individual who furnished the services;
- Billing non-covered or non-chargeable services as covered items;
- Repeatedly violating the participation agreement, assignment agreement, *or* the limitation amount;
- Using another person's Medicare card to obtain medical care;

- Giving false information about provider ownership*; or*
- Using the adjustment payment process to generate fraudulent payments.

Examples of cost report fraud include *(this is not an exhaustive list)*:

- Incorrectly apportioning costs on cost reports;
- Including costs of non-covered services, supplies, or equipment in allowable costs;
- *Providers making a*rrangements with employees, independent contractors, suppliers, and others that appear to be designed primarily to overcharge the program through various devices (commissions, fee splitting) to siphon off or conceal illegal profits;
- Billing Medicare for costs *that were* not incurred or were attributable to non-program activities, other enterprises, or personal expenses;
- Repeatedly including unallowable cost items on a provider's cost report for purposes of establishing a basis for appeal;
- Manipulating statistics to obtain additional payment, such as increasing the square footage in the outpatient areas to maximize payment;
- Claiming bad debts without first genuinely attempting to collect payment;
- *Making improper payments to physicians for c*ertain hospital-based physician arrangements;
- *Paying a*mounts to owners or administrators that have been determined to be excessive in prior cost report settlements;
- *Reporting days improperly* that *result* in an overpayment if not adjusted;
- Depreciat*ing* assets that have been fully depreciated or sold;
- *Using d*epreciation methods not approved by Medicare;
- *Repaying i*nterest expense for loans that *were* for an offset of interest income against the interest expense;
- *Reporting p*rogram data where provider program amounts cannot be supported;
- *Allocating costs improperly* related to organizations that have been determined to be improper*; or*
- *Manipulating a*ccounting.

4.2.2 - Zone Program Integrity Contractor

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs.

The ZPIC is responsible for preventing, detecting, and deterring fraud*, waste, and abuse in both the Medicare program and the Medicaid program through the collaboration of the Medicare-Medicaid Data Match Program (Medi-Medi)*. The ZPIC*:*

- Prevents fraud by identifying program vulnerabilities;
- Proactively identifies incidents of potential *fraud, waste, and abuse* 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*/suppliers*, CMS, OIG, and other sources;.
- Explores all available sources of fraud leads in its *zone*, including the *state Medicaid agency and the Medicaid Fraud Control Unit (*MFCU*);*

- Initiates appropriate administrative actions where there is reliable evidence of fraud, *including, but not limited to, payment suspensions and revocations*;
- Refers cases to the *OIG*/ OI for consideration of civil and criminal prosecution and/or application of administrative sanctions *(see section 4.18 of this chapter, as well as PIM, chapter 8);*
- Refers any necessary provider*/supplier* and beneficiary outreach to the *provider outreach and education (*POE*)* staff at the MAC*;*
- Initiates and maintains networking and outreach activities to ensure effective interaction and exchange of information with internal components as well as outside groups;
- *Partners with state Medicaid Program Integrity units to perform the above activities for the Medi-Medi program; or*
- *Works closely with CMS on joint projects, investigations and other proactive, anti-fraud activities.*

The ZPIC *is* required to use a variety of techniques, both proactive and reactive, to address any potentially fraudulent*, wasteful, or abusive* billing practices *based on the various leads they receive*.

Proactive leads are leads identified or self-initiated by the ZPIC. Examples of proactive leads include, but are not limited to: (1) ZPIC data analysis that uncovers inexplicable aberrancies that indicate potentially fraudulent, wasteful, or abusive billing for specific providers/suppliers; (2) the discovery of a new lead by a ZPIC during a provider/supplier or beneficiary interview; and (3) the combining of information from a variety of sources to create a new lead. The ZPIC shall pursue leads *identified* through data analysis (ZPICs shall follow *PIM* chapter 2, *section* 2.3 for sources of data), the Internet, the Fraud Investigation Database (FID), news media, *industry workgroups, conferences*, etc. For workload reporting purposes*,* the ZPIC shall only identify as proactive those investigations and cases that the ZPIC self-initiated.

The ZPIC shall take prompt action after scrutinizing billing practices, patterns, or trends that may indicate fraudulent billing, *(*i.e., reviewing data for inexplicable aberrancies and relating the aberrancies to specific providers*/suppliers*, identifying "hit and run" providers*/suppliers*, etc.*).*

Fraud leads from any external source (e.g., *LE*, CMS referrals, beneficiary complaints*, and the FPS)* are considered to be reactive and not proactive. However, taking ideas from external sources, such as Fraud Alerts*,* and using them to look for unidentified aberrancies within ZPIC data is proactive.

4.2.2.1 - Organizational Requirements

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs and MACs, as indicated.

ZPIC *program integrity (PI)* managers shall have sufficient authority to guide *PI* activities *and* establish, control, evaluate, and revise fraud-detection procedures to ensure their compliance with Medicare requirements.

ZPIC *PI* manager*s* shall prioritize work coming into the ZPIC to ensure that investigations with the greatest program impact and/or urgency are given the highest priority. *The ZPIC shall prioritize all work on an ongoing basis as new work is received. The ZPIC shall follow PIM, chapter 16 for FPS requirements and prioritization. The ZPIC shall prioritize the top 100 Alert Summary Records (ASRs) in the FPS along with other investigation work based on the PIM prioritization requirements in section 4.2.2.1 of this chapter. The ZPIC shall contact its Contracting Officer's Representative (COR) and Investigations and Audits Group (IAG) Business Function Lead (BFL) if it has any questions or concerns about prioritization of workload.*

The UPIC shall follow the FPS requirements in its UPIC SOW for prioritizing leads provided by CMS, including FPS.

Allegations having the greatest program impact would include investigations cases involving:

- Patient abuse or harm
- Multi-state fraud
- High dollar amounts of potential overpayment
- Likelihood *of* an increase in the amount of fraud or enlargement of a pattern
- *LE* requests for assistance that involve responding to court-imposed deadlines
- *LE* requests for assistance in ongoing investigations that involve national interagency (HHS-DOJ) initiatives or projects.

Note: *The* ZPIC and MAC shall give high priority to fraud*, waste, or abuse complaints* made by Medicare supplemental insurers. If a referral by a Medigap insurer includes investigatory findings indicating fraud stemming from site reviews, beneficiary interviews, and/or medical record reviews, *the* ZPIC shall 1) conduct an immediate data run to determine possible Medicare losses, and 2) refer the case to the OIG.

4.2.2.2 - Liability of Zone Program Integrity Contractor Employees

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs.

Under the terms of their contracts *(refer to 42 CFR* § 421.316(a)*)*, ZPICs, their employees, and professional consultants are protected from criminal or civil liability as a result of the activities they perform under their contracts as long as they use due care. If a ZPIC or any of its employees or consultants *is* named as defendants in a lawsuit, CMS will determine, on a case-by-case basis, whether to request that the U.S. Attorney's office offer legal representation. If the U.S. Attorney's office does not provide legal representation, the ZPIC will be reimbursed for the reasonable cost of legal expenses it incurs in connection with defense of the lawsuit, as long as funds are available and the expenses are otherwise allowable under the terms of the contract.

If a ZPIC is served with a complaint, *the ZPIC* shall immediately contact its chief legal counsel and the *COR*. The ZPIC shall forward the complaint to the *HHS* Office of the *R*egional *C*hief *C*ounsel (*the* CMS regional attorney) who, in turn, will notify the U.S. Attorney*'s office*. The HHS *O*ffice *of the Regional Chief Counsel* and/or the *COR* will notify the ZPIC whether legal representation will be sought from the U.S. Attorney*'s office* prior to the deadline for filing an answer to the complaint.

4.2.2.3 – Anti-Fraud Training

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)
This section applies to ZPICs.

All levels of ZPIC employees shall know the goals and techniques of fraud detection and control in general, and as they relate to their own areas of responsibility and *the level of knowledge required* (i.e., general orientation for new employees and highly technical sessions *for existing staff*). All ZPIC staff shall be adequately qualified for the work of detecting and investigating situations of potential fraud*, waste, and abuse*.

4.2.2.3.1 - Training for Law Enforcement Organizations

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs.

The FBI agents, *OIG,* and DOJ attorneys need to understand Medicare. *The* ZPIC shall conduct special training programs for them upon request. *The* ZPIC should also consider inviting appropriate DOJ, OIG, and FBI personnel to existing programs *for orienting* employees *about* ZPIC operations or *provide the aforementioned personnel with* briefings on specific cases or Medicare issues.

4.2.2.4 - Procedural Requirements

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs and MACs, as indicated.

The MAC personnel conducting each segment of claims adjudication, MR, and professional relations functions shall be aware of their responsibility for identifying potential fraud, waste, or abuse and be familiar with internal procedures for forwarding potential fraud, waste, or abuse instances to the ZPIC. Any area within the MAC (e.g., MR, enrollment, second-level screening staff) that refers potential fraud, waste, and abuse to the ZPIC shall maintain a log of all these referrals. At a minimum, the log shall include the following information: provider/physician/supplier name, beneficiary name, Health Insurance Claim Number (HICN), nature of the referral, date the referral is forwarded to the ZPIC, name and contact information of the individual who made the referral, and the name of the ZPIC to whom the referral was made.

The MAC shall provide written procedures for personnel in various contractor *functions* (claims processing, MR, beneficiary services, *provider/supplier outreach and education (*POE*)*, *cost report* audit, etc.) to help identify potential fraud situations. *The MAC shall i*nclude provisions to ensure that personnel shall*:*

- Refer potential fraud, waste, or abuse *situations* promptly to the ZPIC;
- Forward complaints alleging fraud through the second-level screening staff to the ZPIC;
- Maintain confidentiality of referrals to the ZPIC;
- Forward to the ZPIC *detailed* documentation of telephone or personal contacts involving fraud issues discussed with providers*/suppliers* or provider*/supplier* staff, and retain such information in individual provider*/supplier* files; *and*

The ZPIC shall ensure the performance of the functions below and have written procedures for *implementing* these functions:

Investigations

- Keep educational/warning correspondence with providers*/suppliers* and other fraud documentation concerning specific issues in individual provider*/supplier* files so that ZPICs are able to *easily* retrieve such documentation.

- Maintain documentation on the number of investigations alleging fraud, waste or abuse, the number of cases referred to *the* OIG/OI (and the disposition of those cases), processing time of investigations, and types of violations referred to *the* OIG (e.g., item or service not received, unbundling, waiver of co-payment).
- Conduct investigations (*following a plan of action*) and make the appropriate beneficiary and provider contacts.

Communications/Coordination

- Maintain communication and information flowing between the ZPIC and the MAC MR staff, and as appropriate, MAC audit staff.

- Communicate with the MAC *MR* staff on all findings of overutilization and coordinate with the MAC POE staff to determine what, if any, education has been provided before any *PI* investigation is pursued.
- Obtain and share information on health care fraud issues/fraud investigations among MACs, ZPICs, CMS, and *LE*.
- Coordinate*,* attend*, and actively participate* in fraud-related meetings/conferences and inform, *as well as include* all appropriate parties *in* these meetings/conferences. These meetings/conferences include, but are not limited to, health care *fraud* task force meetings*,* conference calls, *and industry-specific events.*
- Distribute Fraud Alerts *released by CMS* to their staff.
- Serve as a resource to CMS*,* as necessary*;* for example, serve as a resource to CMS on the FID, *provide ideas and feedback on Fraud Alerts and/or vulnerabilities within the Medicare or Medicaid programs.*
- Report to the *COR and IAG BFL all situations* that have been identified where a provider consistently fails to comply with the provisions of the assignment agreement.
- Coordinate and communicate with the MR unit*s* within *the* MACs to avoid duplication of work.

Law Enforcement

- Serve as a reference point for *LE* and other organizations and agencies to contact when they need help or information on Medicare fraud issues and do not know whom to contact.
- *Hire and retain employees who are qualified to testify in a criminal and civil trial when requested by LE.*
- Provide support to *LE* agencies for investigation of potential fraud, including *those* for which an initial referral to *LE* did not originate from the ZPIC.
- Meet (in person or via telephone call) with *the* OIG agents to discuss pending or potential cases, as necessary.
- Meet (in person or *via* telephone) when needed with *the* DOJ to enhance coordination on current or pending cases.
- Furnish all available information upon request to *the* OIG/OI with respect to excluded providers*/suppliers* requesting reinstatement.
- *Notify via e-mail the COR and IAG BFL who will obtain approval or disapproval when the ZPIC is asked to accompany the OIG/OI or any other LE agency onsite to a provider/supplier for the purpose of gathering evidence in a potential fraud case (e.g., executing a search warrant). However, LE must make clear the role of ZPIC personnel in the proposed onsite visit. The potential harm to the case and the safety of ZPIC personnel shall be thoroughly evaluated. The ZPIC personnel shall properly identify themselves as ZPIC employees and under no circumstances shall they represent themselves as LE personnel or special agents. Lastly, under no circumstances shall ZPIC personnel accompany LE in situations where their personal safety is in question.*
- *Maintain independence from LE and do not collect evidence, i.e., request medical records or conduct interviews, at their request.*

Training

- Work with the *COR and IAG BFL* to develop and organize external programs and perform training*,* as appropriate, for *LE*, ombudsmen, grantees (e.g., S*enior* M*edicare* P*atrol*s)*,* and other CMS health care partners (e.g., *Administration on Aging (*AoA*)*, *s*tate MFCU*s*).

- Help to develop fraud-related outreach materials (e.g., pamphlets, brochures, videos) in cooperation with beneficiary services and/or provider relations departments of the MACs for use in their training. Submit written outreach material to the *COR* and *IAG BFL* for clearance.
- Assist in *preparing and developing* fraud-related articles for MAC newsletters/bulletins. *Once completed, the* ZPIC shall *submit such materials to the* following *email* address*: CPIFraudRelatedLeads@cms.hhs.gov, with a copy to the CORs and IAG BFLs*.
- Provide resources and training for the development of *existing employees and new hires*.

The MACs *shall* ensure the performance of the functions below and have written procedures for these functions:

- Ensure no payments are made for items or services ordered, referred, or furnished by an individual or entity following the effective date of exclusion (*refer to § 4.19*, for exceptions).
- Ensure all instances where an excluded individual or entity that submits claims for which payment may not be made after the effective date of the exclusion are reported to the OIG (*refer to* PIM*,* chapter *8*,).
- Ensure no payments are made *to a Medicare provider/supplier that employs an excluded* individual or entity.

4.2.2.4.1 - Maintain Controlled Filing System and Documentation

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

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

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

- All incoming correspondence or other documentation associated with an investigation contains the same file number and is placed in a folder containing the original investigation material.
- Investigation files are adequately documented to provide an accurate and complete picture of the investigative effort.
- All contacts are clearly and appropriately documented.
- Each file contains the initial prioritization assigned and all updates.

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

The ZPIC shall establish an internal monitoring and investigation review system to ensure the adequacy and timeliness of fraud*, waste,* and abuse activities.

4.2.2.6 – *Program* Integrity Security Requirements

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs.

To ensure a high level of security for the ZPIC function*s*, the ZPIC shall develop, implement, operate, and maintain security policies and procedures that meet and conform to the requirements of the Business Partners *System* Security Manual (BPSSM) and the *CMS Informational Security Acceptable Risk Safeguards (ISARS)*. Further, the ZPIC shall adequately inform and train all ZPIC employees to follow ZPIC security policies and procedures so *that* the information the ZPIC obtain is confidential.

Note: *The* data ZPICs collect in *administering* ZPIC contracts belong to CMS. Thus, the ZPICs collect and use individually identifiable information on behalf of the Medicare program to routinely perform the business functions necessary for administ*ering* the Medicare program, such as *MR* and program integrity activities to prevent fraud*, waste,* and abuse. Consequently, any disclosure of individually identifiable information without prior consent from the individual to whom the information pertains, or without statutory or contract authority, requires CMS' prior approval.

This section discusses broad security requirements that ZPICs shall follow. *The* requirements listed below are in the BPSSM or *ARS. There are several exceptions. The first is requirement A (concerning ZPIC operations), which addresses several broad requirements; CMS has included requirement A here for emphasis and clarification. Two others are in requirement B (concerning sensitive information) and requirement G (concerning telephone security). Requirements B and G relate to security issues that are not systems related and are not in the BPSSM.*

A. Zone Program Integrity Contractor Operations

- The ZPIC shall conduct their activities in areas not accessible to the general public.
- The ZPIC shall completely segregate *itself* from all other operations. Segregation shall include floor-to-ceiling walls and/or other measures described in *ARS Appendix B PE-3 and CMS-2* that prevent unauthorized persons access to or inadvertent observation of sensitive and investigative information.
- Other requirements regarding ZPIC operations shall include sections 3.1, 3.1.2, 4.2, 4.2.5, and 4.2.6 of the BPSSM.

B. Handling and Physical Security of Sensitive and Investigative Material

Refer to ARS Appendix B PE-3 and CMS-1 for definitions of sensitive and investigative material.

In addition, *the* ZPIC shall follow the requirements provided below:

- Establish a policy that employees shall discuss specific allegations of fraud only within the context of their professional duties and only with those who have a valid need to know, which include*s (this is not an exhaustive list)*:
    - Appropriate CMS personnel
    - ZPIC staff
    - MAC MR staff
    - ZPIC or MAC audit staff
    - ZPIC or MAC data analysis staff
    - ZPIC or MAC senior management
    - ZPIC or MAC corporate counsel
- The *ARSs* require that:
    - The following workstation security requirements are specified and implemented: (1) what workstation functions can be performed, (2) the manner in which those functions are to be performed, *and* (3) the physical attributes of the surrounding*s* of a specific workstation or class of workstation that can access sensitive CMS information. CMS requires that for ZPICs all

local workstations as well as workstations used at home by ZPICs comply with these requirements.

- If ZPIC employees are authorized to work at home on sensitive data, they *shall* observe the same security practices that they observe at the office. These *shall* address such items as viruses, *virtual private networks*, and protection of sensitive data*, including* printed documents.
- Users are prohibited from installing desktop modems.
- The connection of portable computing or portable network devices on the CMS claims processing network is restricted to approved devices only. Removable hard drives and/or a *Federal Information Processing Standards (*FIPS*)*-approved method of cryptography shall be employed to protect information residing on portable and mobile information systems.
- Alternate work sites are those areas where employees, subcontractors, consultants, auditors, etc. perform work associated duties. The most common alternate work site is an employee's home. However, there may be other alternate work sites such as training centers, specialized work areas, processing centers, etc. For alternate work site equipment controls, (1) only CMS Business Partner-owned computers and software are used to process, access, and store sensitive information; (2) a specific room or area that has the appropriate space and facilities is used; (3) means are available to facilitate communication with the managers or other members of the Business Partner Security staff in case of security problems; (4) locking file cabinets or desk drawers; (5) "locking hardware" to secure IT equipment to larger objects such as desks or tables; and (6) smaller Business Partner-owned equipment is locked in a storage cabinet or desk when not in use. If wireless networks are used at alternate work sites, wireless base stations are placed away from outside walls to minimize transmission of data outside of the building.

The ZPIC shall also adhere to the following:

- Ensure the mailroom, general correspondence, and telephone inquiries procedures maintain confidentiality whenever the ZPIC receives correspondence, telephone calls, or other communication alleging fraud. Further, all internal written operating procedures shall clearly state security procedures.
- Direct mailroom staff not to open ZPIC mail in the mailroom unless the ZPIC has requested the mailroom do so for safety and health precautions. Alternately, if mailroom staff opens ZPIC mail, mailroom staff shall not read the contents.
- For mail processing sites separate from the ZPIC, the ZPIC shall minimize the handling of ZPIC mail by multiple parties before delivery to the ZPIC.
- The ZPIC shall mark mail to *CMS Central Office* or *to* another ZPIC "personal and confidential" and address it to a specific person.
- Where more specialized instructions do not prohibit ZPIC employees, *they* may retain sensitive and investigative materials at their desks, in office work baskets, and at other points in the office during the course of the normal work day. Regardless of other requirements, the employee*s* shall restrict access to sensitive and investigative materials, and ZPIC staff shall not leave such material unattended.
- *The* ZPIC staff shall safeguard all sensitive or investigative material when *the materials are being transported or sent by ZPIC staff*.
- The ZPIC shall maintain a controlled filing system (*refer to section 4.2.2.4.1*).

C. Designation of a Security Officer

The security officer shall take such action as is necessary to correct breaches of the security standards and to prevent recurrence of the breaches. In addition, the security officer shall document the action taken and maintain that documentation for at least *seven (*7*)* years. Actions shall include:

- Within one *(1)* hour of discovering a security incident, clearly and accurately report the incident following BPSSM requirements for reporting of security incidents. For purposes of this requirement, a security incident is the same as the definition in *section* 3.6 *of the BPSSM*, Incident Reporting and Response.
- Specifically, the report shall address the following where appropriate:
  - Types of information about beneficiaries shall at a minimum address whether the compromised information includes name, address, HICN*s*, and date of birth*;*
  - Types of information about providers*/suppliers* shall at a minimum address if the compromised information includes name, address, and provider*/supplier* ID*;*
  - Whether *LE* is investigating any of the providers*/suppliers* with compromised information*;* and
  - Police reports.
- Provide additional information that CMS requests within 72 hours of the request.
- If CMS requests, issue a Fraud Alert to all CMS Medicare contractors *within 72 hours of the discovery that the data was compromised,* listing the HICNs and provider*/supplier* IDs that were compromised.
- Within 72 hours of discovery of a security incident, when feasible, review all security measures and revise them if necessary so they are adequate to protect data against physical or electronic theft.

Refer to section 3.1 of the BPSSM and Attachment 1 *of* this manual section (letter from Director, Office of Financial Management, concerning security and confidentiality of ZPIC data) for additional requirements.

D. Staffing of the Zone Program Integrity Contractor and Security Training

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

At the point the ZPIC makes a hiring decision for a ZPIC position, and prior to the selected person's starting work, the ZPIC shall require the proposed candidate to fill out a conflict of interest declaration, as well as a confidentiality *s*tatement.

Annually, the ZPIC*s* shall require existing employees to complete a conflict of interest declaration*,* as well as a confidentiality *s*tatement.

The ZPIC*s* shall not employ temporary employees, such as those from temporary agencies, *or* students (nonpaid or interns).

At least once a year, the ZPIC*s* shall thoroughly explain to and discuss with employees *the* special security considerations under which the ZPIC operates. Further, this training shall emphasize that in no instance shall employees disclose sensitive or investigative information*,* even in casual conversation. *The ZPIC shall ensure that employees understand the training provided.*

Refer to section 2.0 of the BPSSM and *ARS Appendix B AT-2, AT-3, AT-4, SA-6, MA-5.0, PE-5.CMS.1, IR2-2.2, CP 3.1, CP 3.2, CP 3.3, and SA 3.CMS.1* for additional training requirements.

E. Access to *Zone Program Integrity Contractor* Information

Refer to section 2.3.4 of the BPSSM for requirements regarding access to ZPIC information.

The ZPIC shall notify the OIG if parties without a need to know are asking inappropriate questions regarding any investigations. The ZPIC*s* shall refer all requests from the press related to the Medicare

Integrity Program to the CMS contracting officer *with a copy to the CORs and IAG BFLs* for approval prior to release. This includes, but is not limited to, contractor initiated press releases, media questions, media interviews, and Internet postings.

F. Computer Security

Refer to section 4.1.1 of the BPSSM for the computer security requirements.

G. Telephone *and Fax* Security

The ZPIC*s* shall implement phone security practices. The ZPIC*s* shall discuss investigations only with those individuals *who* need to know the information and shall not divulge information to individuals not known to the ZPIC involved in the investigation of the related issue.

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

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

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

4.3 – Medical Review for *Program* Integrity Purposes

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

Medical Review (MR) for Program Integrity (PI) is one of the parallel strategies of the Medicare Integrity Program (MIP) to encourage the early detection of fraud, waste, and abuse. The primary task of the ZPIC is to identify suspected fraud, develop investigations and cases thoroughly and in a timely manner, and take immediate action to ensure that Medicare Trust Fund monies are not inappropriately paid out and that any improper payments are identified. For this reason, it is recommended that MR is integrated early into the development of the investigative process. The focus of PI MR includes, but is not limited to:

- *Possible falsification or other evidence of alterations of medical record documentation including, but not limited to: obliterated sections; missing pages, inserted pages, white out; and excessive late entries;*
- *Evidence that the service billed for was actually provided and/or provided as billed; or,*
- *Patterns and trends that may indicate potential fraud, waste, and abuse.*

The statutory authority for the MR program includes the following sections of the Social Security Act (the Act):

- *Section 1833(e), which states in part "...no payment shall be made to any provider... unless there has been furnished such information as may be necessary in order to determine the amounts due such provider ...;"*
- *Section 1842(a)(2)(B), which requires MACs to "assist in the application of safeguards against unnecessary utilization of services furnished by providers ...; "*

- *Section 1862(a)(1), which states no Medicare payment shall be made for expenses incurred for items or services that "are not reasonable and necessary for the diagnosis or treatment of illness or injury or to improve the functioning of a malformed body member;"*

The remainder of Section 1862(a), which describes all statutory exclusions from coverage;

- *Section 1893(b)(1) establishes the Medicare Integrity Program, which allows contractors to review activities of providers of services or other individuals and entities furnishing items and services for which payment may be made under this title (including skilled nursing facilities and home health agencies), including medical and utilization review and fraud review (employing similar standards, processes, and technologies used by private health plans, including equipment and software technologies which surpass the capability of the equipment and technologies. . .")*
- *Sections 1812, 1861, and 1832, which describe the Medicare benefit categories; and*
- *Sections 1874, 1816, and 1842, which provide further authority.*

The regulatory authority for the MR program rests in:

- *42 CFR § 421.100 for intermediaries.*
- *42 CFR § 421.200 for carriers.*
- *42 CFR § 421.400 for MACs.*

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

The ZPIC and *the* MAC MR units shall have ongoing discussions and close working relationships regarding situations identified that may be signs of potential *fraud, waste, or abuse*. MACs shall also include the cost report audit unit in the on-going discussions. MAC MR staff shall coordinate and communicate with their associated ZPIC*s* to ensure coordination of efforts, to prevent inappropriate duplication of review activities, and to assure contacts made by the MAC are not in conflict with *program* integrity related activities*, as defined by the Joint Operating Agreement (JOA)*.

It is essential that MR is integrated early in the investigative plan of action to facilitate the timeliness of the investigative process. Before deploying significant MR resources to examine claims identified as potentially fraudulent, the ZPIC may perform a limited prepayment MR to help identify signs of potential fraud, waste, or abuse. The general recommendation for a provider/supplier specific edit would be to limit the prepayment MR to specific procedure codes, a specific number of claims, or based on a particular subset of beneficiaries identified through the ZPIC's analysis. Another option may be for the ZPIC to perform a MR probe to validate the data analysis or allegation by selecting a small representative sample of claims. The general recommendation for a provider/supplier-specific probe sample is 20-40 claims. This sample size should be sufficient to determine the need for additional prepayment or post-payment MR actions. MR resources shall be used efficiently and not cause a delay in the investigative process. In addition, development of an investigation shall continue while the contractor is awaiting the results of the MR.

A. Referrals from the *Medicare Administrative Contractor* to the *Zone Program Integrity Contractor*

If a provider*/supplier* 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 MAC MR unit personnel shall discuss this *matter* with the *ZPIC*. If the *ZPIC* agrees that there is potential *fraud*, the *MAC* MR unit shall then make a referral to the *ZPIC* for investigation.

Provider/*supplier* documentation that shows a pattern of repeated misconduct or conduct that is clearly abusive or potentially fraudulent, despite provider/*supplier* education and direct contact with the provider/*supplier* to explain identified errors, shall be referred to the *ZPIC*.

The focus of MAC MR is to reduce the error rate through MR and provider/supplier notification and feedback, whereas ZPIC MR for PI focuses on addressing situations of potential fraud, waste, and abuse.

B. Referrals from the *Zone Program Integrity Contractor* to the Medical Review Unit and Other Units

The *ZPICs* are also responsible for preventing and minimizing the opportunity for fraud. The *ZPICs* shall identify procedures that may make Medicare vulnerable to *questionable billing or improper practices* and take appropriate action.
CMS has implemented recurring edit modules in all claims processing systems to allow *ZPICs* and/or CMS to monitor specific beneficiary and/or provider/*supplier* numbers and other claims criteria. When appropriate, the *ZPIC* may request the MAC to install a prepayment or auto-denial edit. The MACs shall comply with requests from *ZPICs* and/or CMS to implement those edits. The MACs shall implement parameters for those edits/audits within *the timeframe established in the MAC and ZPIC JOA, which shall not exceed more than 15 business* days.

C. *Program* Integrity/Medical Review Determinations

When *MAC* MR staff is reviewing a medical record for MR purposes, *its* focus is on making a coverage and/or coding determination. However, when *ZPIC* staff *is* performing *MR for PI purposes*, *its* focus may be different (e.g., looking for possible falsification). *The ZPIC shall follow all chapters of the PIM as applicable unless otherwise instructed in this chapter and/or in its Umbrella Statement of Work (USOW).* Chapter 3 *of the PIM* outlines the procedures to be followed to make coverage and coding determinations.

1. The *ZPIC* shall maintain current references to support *MR* determinations. *The review staff shall be familiar with the below references and be able to track requirements in the internal review guidelines back to the statute or manual. References include,* but *are* not limited to:
   - *CFRs*;
   - CMS Internet Only Manuals (IOMs);
   - Local coverage determinations (LCDs);
   - *National coverage determinations (NCDs); and*
   - Internal review guidelines (sometimes defined as desktop procedures).

2. The *ZPIC* shall have specific review parameters and guidelines established for the identified claims. Each claim shall be evaluated using the same review guidelines. The claim and the medical record shall be linked by patient name, *HICN*, diagnosis, *Internal Control Number (*ICN*)*, and procedure. The *ZPIC* shall have access to provider/*supplier* tracking systems from *MR*. The information on the tracking systems *shall* be used for comparison to *ZPIC* findings. The *ZPIC* shall also consider that the *MR* department may have established internal guidelines (see PIM, chapter 3).

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

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

5. The *ZPIC* shall determine if patterns and/or trends exist in the medical record *that* may indicate potential fraud, waste, or *abuse or demonstrate potential patient harm*. Examples include, but are not limited to:

- The medical records tend to have obvious or nearly identical documentation.
- In reviews that cover a sequence of codes (*e.g.,* evaluation *and* management codes, therapies, radiology), evidence *may exist* of a trend to use *with greater-frequency than would be expected* the high-end *billing* codes *representing higher level services.*
- In a provider*/supplier* review, *a pattern* may be *identified* of billing more hours of care than would normally be expected on a given workday.
- The medical records indicate a procedure is being done more frequently than prescribed per suggested CMS guidance or industry standards of care, resulting in potential situations of patient harm.

6. The *ZPIC* shall evaluate the medical record for evidence of alterations including, but not limited to, obliterated sections, missing pages, inserted pages, white out, and excessive late entries. *The ZPIC shall not consider undated or unsigned entries handwritten in the margin of a document. These entries shall be excluded from consideration when performing medical review. See chapter 3 for recordkeeping principles.*

7. The *ZPIC* shall document errors found and communicate these to the provider*/supplier* in *writing* when the *ZPIC's* review does not find evidence of *questionable billing or improper practices*. A referral may be made to the POE staff at the MAC for additional provider*/supplier* education and follow up, if appropriate *(see PIM, chapter 3).*

8. The *ZPIC* shall *adjust the service*, in part or in whole, depending upon the service under review, when medical records*/documentation* do not support services billed by the provider*/supplier*.

9. The *ZPIC* shall thoroughly document the rationale utilized to make the *MR* decision.

D. Quality Assurance

Quality assurance activities shall ensure that each element is being performed consistently and accurately throughout the *ZPIC's* MR for *PI* program. In addition, the *ZPIC* shall have in place procedures for continuous quality improvement *in order to* continually improve the effectiveness of their processes.

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

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

3. The *ZPIC* shall have an objective process to assign staff to review projects, ensuring that the correct level of expertise is available. For example, situations dealing with therapy issues may include review by an appropriate therapist or use of a therapist as a consultant to develop internal guidelines. Situations with complicated or questionable medical issues, or where no policy exists, may require a physician consultant (medical director or outside consultant).

4. The *ZPIC* shall develop a system to address how it will monitor and maintain accuracy in decision making (inter-reviewer reliability) as referenced in chapter *3 of the PIM. The ZPIC shall establish a Quality Improvement (QI) process that verifies the accuracy of MR decisions made by licensed health care professionals. ZPICs shall include inter-rater reliability and/or peer-review assessments in their QI process and shall report these results as directed by CMS.*

5. When the *ZPIC* evaluation results identify the need for prepayment edit placement at the MAC, the *ZPIC* shall have a system in place to evaluate the effectiveness of those edits on an ongoing basis as development continues *The MAC may provide the claims data necessary to the ZPIC to evaluate edits submitted at the request of the ZPIC. The evaluation of edits shall consider the timing and staffing needs for reviews. The ZPIC may submit an inquiry to the MAC to verify that a new edit is accomplishing its objective of selecting claims for MR 30 business days after an edit has been implemented or placed into production. The ZPIC shall use data analysis of the selected provider's claims history to verify possible changes in billing patterns.*

   Automated edits shall be evaluated annually.

   Prepayment edits shall be evaluated on a quarterly basis. They shall be analyzed in conjunction with data analysis to confirm or re-establish priorities. For example, a prepayment edit is implemented to stop all claims with a specific diagnostic/procedure code and the provider stops submitting claims with that code to circumvent the edit. Data analysis shall be used to identify if the provider's general billing pattern has changed in volume and/or to another/similar code that may need to be considered/evaluated to revise the current edit in question and/or expansion of the current investigation.

4.4.1 - Requests for Information from Outside Organizations

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs.

Federal*, s*tate*,* and local *LE* agencies may seek beneficiary and provider*/supplier* information to further their investigations or prosecutions of individuals or businesses alleged to have committed health care fraud and other crimes for which medical records may be sought as evidence. When these agencies request that a ZPIC disclose beneficiary records or provider*/supplier* information, the responsive disclosure shall comply with applicable *f*ederal law as required by the *Health Insurance Portability and Accountability Act of 1996 (*HIPAA*)* Business Associate provision of the ZPIC*'s* contract. Federal law will dictate whether, and how much, requested information can be disclosed. *The determination regarding* disclosure will be contingent on the purpose for which it is sought and whether information is sought about beneficiaries or providers*/suppliers*. *For example, c*ertain general information *that* does not include specific beneficiary identifiers may be shared with a broader community, including private insurers. *T*he *information may include that of a* general nature of how fraudulent practices were detected, the actions being taken, and aggregated data showing trends and/or patterns.

The ZPIC may release information, in accordance with the requirements specified in Sections A – G below, to the following organizations:

- *Other ZPICs*
- *Qualified Independent Contractors (QICs)*
- *Quality Improvement Organizations (QIOs)*
- *State Attorneys General and State Agencies*
- *Medicaid Fraud Control Units (MFCUs)*
- *OIG*
- *DOJ*
- *FBI*

Requests for information from entities not listed above shall be submitted to the COR for approval, with a copy to the IAG BFL.

In deciding to share information voluntarily or in response to outside requests, the ZPIC shall carefully review each request to ensure that disclosure would not violate the requirements of the Privacy Act of 1974 (5 U.S.C. *§*552a) and/or the Privacy Rule (45 CFR, Parts 160 and 164) implemented under the HIPAA. Both

the Privacy Act and the *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, *both statutes* provide individuals with the right to know with whom their personal information has been shared, necessitat*ing* the tracking of any disclosures of information by the ZPIC. *The* ZPIC *shall direct* questions concerning what information may be disclosed under the Privacy Act or Privacy Rule to *the CMS R*egional *O*ffice 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 *[PHI]*) by organizations subject to the Privacy Rule (which are called "covered entities"). As "business associate*s*" of CMS, ZPICs are contractually required to comply with the HIPAA Privacy Rule. The Privacy Rule restricts the disclosure of any information, in any form, that can identify the recipient of medical services*;* unless that disclosure is expressly permitted under the Privacy Rule. Two of the circumstances in which the Privacy Rule allows disclosure are for "health oversight activities" (45 CFR *§*164.512(d)) and *for* "law enforcement purposes" (45 CFR *§*164.512 (f)), provided the disclosure meets all the relevant prerequisite procedural requirements in those subsections. Generally, *PHI* may be disclosed to a health oversight agency (as defined in 45 CFR *§*164.501) for purposes of health oversight activities authorized by law, including administrative, civil, and criminal investigations necessary for appropriate oversight of the health care system (45 CFR *§*164.512(d)). The DOJ, through its United States Attorneys' Offices and its headquarters-level litigating divisions*;* the FBI*;* the *HHS* OIG*;* and other *f*ederal, *s*tate, or local enforcement agencies, are acting in the capacity of health oversight agencies when they investigate fraud against Medicare, Medicaid, or other health care insurers or programs.

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

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

Information from some systems of records may be released only if the disclosure would be consistent with "routine uses" that CMS has issued and published. Routine uses specify who may be given the information and the basis or reason for access that must exist. Routine uses vary by the specified system of records, and a decision concerning the applicability of a routine use lies solely in the purview of the system's manager for each system of records. In instances where information is released as a routine use, the Privacy Act and Privacy Rule remain applicable. For example, the *HHS* has published a routine use *that* permits the disclosure of personal information concerning individuals to the *DOJ*, as needed for the evaluation of potential violations of civil or criminal law and for detecting, discovering, investigating, litigating, addressing, or prosecuting a violation or potential violation of law, in health benefits programs administered by CMS. *Refer to* 63 Fed. Reg. 38414 (July 16, 1998).

The 1994 Agreement and the 2003 form letter (refer to 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 (1) of 12 disclosure provisions apply. Two of these provisions, the "routine use" provision and/or another "law enforcement" provision, may apply to requests from the DOJ and/or the FBI.

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

Both the Fiscal Intermediary Shared System (FISS) #8 and #10, the Multi-Carrier System (MCS), and the VIPS Medicare System (VMS) 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, such 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 (1) of the 11 other exceptions to the Privacy Act applies.

The LE provision may apply to requests from the DOJ and/or the 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 LE 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 that maintains the record specifying the particular portion desired and the LE activity for which the record is sought."

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

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

A. Requests from Private, Non-Law Enforcement Agencies

Generally, ZPIC*s* 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 *may be released* to an outside entity, *the* ZPIC shall contact *its COR and IAG BFL* for further guidance.

B. Requests from *Other* Zone Program Integrity Contractors

The ZPIC*s* may furnish requested specific information *concerning* ongoing fraud investigations and individually identifiable *PHI* to any ZPIC or MAC. ZPICs and MACs are "business associates" of CMS

under the Privacy Rule and thus are permitted to exchange information necessary to conduct health care operations. If the request concerns investigations already referred to the OIG/OI, *the* ZPIC shall *notify the OIG/OI of the* request *for information received from another ZPIC and notify the requesting ZPIC that the case has been referred to the OIG/OI.*

C. Requests for Information from Qualified Independent Contractors

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

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

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

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

D. *Requests from* Quality Improvement Organizations and State Survey and Certification Agencies

The ZPIC may furnish requested specific information *concerning* ongoing fraud investigations *containing personally* identifiable *information* to the QIOs and *s*tate 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, ZPIC*s* shall refer the requestor to the OIG/OI.

E. *Requests from* State Attorneys General and State Agencies

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

F. Request*s* from Medicaid Fraud Control Units

Under current Privacy Act requirements applicable to program integrity investigations, *the* ZPIC may respond to requests from MFCUs for information on current investigations. Releases of information to MFCUs in connection with their responsibility to investigate, prosecute, enforce, or implement a *s*tate 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). *Refer to* subsection H below for further information regarding the Privacy Act requirements. If individually identifiable *PHI* is requested, the disclosure shall

comply with the Privacy Rule. *Refer to* subsection H below and PIM Exhibit 25 for guidance on how requests should be structured to comply with the Privacy Rule.

The ZPIC may, at *its* discretion, share *PIM* Exhibit 25 with the requestor*s* as a template to assist them in preparing their request. If the request concerns cases already referred to the OIG/OI, *the* ZPIC shall refer the requestor to the OIG/OI.

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

The ZPIC shall provide the OIG/OI with requested information and shall maintain cost information related to fulfilling these requests. *A request for information shall consist of requests to run data for the OIG, extract of records, or a request to furnish any documentation or reports (see below for requests for assistance).* Such requested information may include *LE* requests for voluntary refund data (*see section* 4.16 *of this chapter*). *The ZPIC shall not fulfill a request if there is a substantial impact (i.e., 40 hours or more) on the budget without prior COR approval. The ZPIC shall copy the IAG BFL on these requests for approval from the COR.* 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*/supplier*. The request shall be completed with the utmost urgency. Priority I requests shall be fulfilled within thirty (30) *calendar* days when the information or material is contained in the ZPIC*'s* files unless an exception exists as described below.
The ZPIC shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested *within 30 calendar days or sooner, when possible*. *The MAC shall furnish requested information to the ZPIC within 20 calendar days of receipt of the request from the ZPIC unless there are extenuating circumstances. The MAC shall communicate any extenuating circumstances to the ZPIC and the MAC COR as soon as they become known. The ZPIC shall communicate these extenuating circumstances to its COR.*
The ZPIC shall follow up with other contractors, and document all communication with contractors to ensure the request is not delayed unnecessarily. *If extenuating circumstances exist that prevent the ZPIC from meeting the thirty (30) day timeframe, the ZPIC shall inform the requestor what, if any, portion of the request can be provided within thirty (30) days.* The ZPIC shall notify the requesting office as soon as possible (but not later than thirty (30) days) after receiving the request. The ZPIC shall also document all communication with the requesting office regarding the delay, and shall include an estimate of when all requested information will be supplied.
If the request requires that the ZPIC access National Claims History (NCH) using Data Extract Software (DESY), the thirty (30) day timeframe for Priority I requests does not apply.

Priority II – This type of request is less critical than a Priority I request. *A request for information shall consist of requests to run data for the OIG, extract of records, or a request to furnish any documentation or reports (see below for requests for assistance).* Based on the review of its available resources, the ZPIC shall inform the requestor what, if any, portion of the request can be provided. The ZPIC shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested.
The *ZPICs* shall respond to such requests within 45 calendar days *or sooner*, when possible. *The MAC shall furnish requested information to the ZPIC within 30 calendar days of receipt of the request from the ZPIC unless there are extenuating circumstances. The MAC shall communicate any extenuating circumstances to the ZPIC and the MAC COR as soon as they become known. The ZPIC shall communicate these extenuating circumstances to its COR.* The ZPIC shall follow up with other contractors, and document all communication with contractors to ensure the request is not delayed unnecessarily. *If extenuating circumstances exist that prevent the ZPIC from meeting the 45-day timeframe, the ZPIC shall inform the requestor what, if any, portion of the request can be provided within 45 calendar days.* The ZPIC shall notify the requesting office as soon as possible (but not later than 45 *calendar* days) after receiving the request. The ZPIC shall also document all communication with the requesting office regarding the delay, and shall include an estimate of when all requested information will be supplied.
Request for Assistance – *A LE request for assistance (RFA) is a type of request for information and shall consist of any LE requests that do not include running data and reports, but include requests such as the review and interpretation of medical records/medical documentation, interpretation of policies, and*

reviewing cost reports. The timeframes for RFIs specified in Priority I and II do not apply to RFAs. Due dates shall be negotiated with the requesting entity and documented appropriately along with the reasons for not meeting the agreed upon timeframes. The ZPIC shall contact the COR if an agreement cannot be reached on the timeframe for completion. Disclosures of information to the OIG shall comply with the Privacy Rule and Privacy Act. *When the OIG makes a data request, the ZPIC shall track these requests and document the following: (1) nature/purpose of the disclosure (cite a specific investigation and have a general description); (2) what information was disclosed; and (3) name of the individual and the agency. The aforementioned information shall be maintained in a secure file and made available to CMS upon request through a secure means.*

CMS has established a level of effort limit of 40 hours for any individual request for support (Requests for Information and Requests for Assistance). If the estimated level of effort to fulfill any one request is likely to meet or exceed this figure, the ZPIC shall contact its COR for approval to proceed. A CMS representative will contact the OIG to explore the feasibility of other data search and/or production options.

The ZPIC shall obtain approval from the COR regarding requests started by the ZPIC that they subsequently anticipate will exceed that 40-hour level of effort. The ZPIC shall not exceed the 40-hour level of effort until it receives COR approval.

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

In April 1994, CMS entered into an interagency agreement with the *OIG* and the DOJ that permitted ZPICs to furnish information *that previously had to be routed through OIG (refer to PIM Exhibit 16)* including data related to the investigation of health care fraud matters directly to *the* DOJ that previously had to be routed through OIG (*refer to* PIM Exhibit 35). This agreement was supplemented on April 11, 2003, when in order to comply with the HIPAA Privacy Rule, *the* DOJ issued procedures, guidance, and a form letter for obtaining information (*refer to* PIM Exhibit 25). CMS and *the* DOJ have agreed that *the* DOJ*'s* requests for individually identifiable health information will follow the procedures that appear on the form letter (*refer to* 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 requestor indicates he or she is pursuing an MSP fraud matter.

The PIM Exhibit 25 contains the entire document issued by the DOJ on April 11, 2003. *The* ZPIC shall familiarize *itself* with the instructions contained in this document. Data requests for individually identifiable *PHI* related to the investigation of health care fraud matters will come directly from those individuals at *the* FBI or *the* DOJ who are involved in the work of the health care oversight agency (including, for example, FBI agents, *Assistant United States Attorneys (*AUSAs*)*, or designee*s* such as analyst*s*, auditor*s,* investigator*s*, or paralegal*s*). For example, data may be sought to assess allegations of fraud; examine billing patterns; ascertain dollar losses to the Medicare program for a procedure, service, or time period; determine the nature and extent of a provider's*/supplier's* voluntary refund(s); or conduct a random sample of claims for *MR*. The *LE* agency should begin by consulting with the appropriate Medicare contractor (usually the ZPIC, but possibly also the MAC) or CMS to discuss the purpose or goal of the data request. Requests for cost report audits and/or associated documents shall be referred directly to the appropriate MAC.

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

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

If *the* DOJ confirms that claims data are necessary, *the* DOJ will prepare a formal request letter to the ZPIC with existing DOJ guidance (Exhibit *15*).

The ZPIC *shall* provide data to *the* DOJ, when feasible, in a format to be agreed upon by the ZPIC and *the* DOJ. Expected time frames for fulfilling *the* DOJ claims-level data requests will depend on the respective source(s) and duration of time for which data are sought, with the exception of *e*mergency *r*equests, which require coordination with Headquarters, *the* DOJ, and CMS staff. *T*hese are as follows:

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

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*/supplier*. *A request for information shall consist of requests to run data for the DOJ, extract of records, or a request to furnish any documentation or reports (see below for requests for assistance).* The request shall be completed with the utmost urgency. Priority I requests shall be fulfilled within thirty (30) *calendar* days when the information or material is contained in the *ZPIC's files* unless an exception exists as described below.
The ZPIC shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested *within 30 calendar days or sooner, when possible*. *The MAC shall furnish requested information to the ZPIC within 20 calendar days of receipt of the request from the ZPIC unless there are extenuating circumstances. The MAC shall communicate any extenuating circumstances to the ZPIC and the MAC COR as soon as they become known. The ZPIC shall communicate these extenuating circumstances to its COR.* The ZPIC shall follow up with other contractors, and document all communication with contractors to ensure the request is not delayed unnecessarily. *If extenuating circumstances exist that prevent the ZPIC from meeting the thirty (30) day timeframe, the ZPIC shall inform the requestor what, if any, portion of the request can be provided within thirty (30) days.* The ZPIC shall notify the requesting office as soon as possible (but not later than thirty (30) days) after receiving the request. The ZPIC shall also document all communication with the requesting office regarding the delay, and shall include an estimate of when all requested information will be supplied.

If the request requires that the ZPIC access NCH using DESY, the thirty (30) day timeframe for Priority I requests does not apply.

Priority II Requests – This type of request is less critical than a Priority I request. *A request for information shall consist of requests to run data for the DOJ, extract of records, or a request to furnish any documentation or reports (see below for requests for assistance).* Based on the review of its available resources, the ZPIC shall inform the requestor what, if any, portion of the request can be provided. The ZPIC shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested.

The *ZPIC* shall respond to such requests within 45 calendar days *or sooner*, when possible. *The MAC shall furnish requested information to the ZPIC within 30 calendar days of receipt of the request from the ZPIC unless there are extenuating circumstances. The MAC shall communicate any extenuating circumstances to the ZPIC and the MAC COR as soon as they become known. The ZPIC shall communicate these extenuating circumstances to their COR. The ZPIC shall follow up with other contractors, and document all communication with contractors to ensure the request is not delayed unnecessarily. If extenuating circumstances exist that prevent the ZPIC from meeting the 45-day timeframe, the ZPIC shall inform the requestor what, if any, portion of the request can be provided within 45 calendar days. The ZPIC shall notify the requesting office as soon as possible (but not later than 45 calendar days) after receiving the request.* The ZPIC shall *also* document *all* communication with *the requesting office regarding the delay, and shall include an estimate of when all requested information will be supplied.*

Request for Assistance – *A LE request for assistance (RFA) is a type of request for information and shall consist of any LE requests that do not include running data and reports, but include requests such as the review and interpretation of medical records/medical documentation, interpretation of policies, and reviewing cost reports. The timeframes for RFIs specified in Priority I and II do not apply to RFAs. Due dates shall be negotiated with the requesting entity and documented appropriately along with the reasons*

for not meeting the agreed upon timeframes. The ZPIC shall contact the COR if an agreement cannot be reached on the timeframe for completion.

Disclosures of information to the DOJ shall comply with the Privacy Rule and Privacy Act. When DOJ makes a data request, the ZPIC shall track these requests and document the following: (1) nature/purpose of the disclosure (cite a specific investigation and have a general description); (2) what information was disclosed; and (3) name of the individual and the agency. The aforementioned information shall be maintained in a secure file and made available to CMS upon request through a secure means.

CMS has established a level of effort limit of 40 hours for any individual request for support (RFIs and RFAs). If the estimated level of effort to fulfill any one request is likely to meet or exceed this figure, the program integrity contractor shall contact its COR for approval to proceed. A CMS representative will contact the OIG to explore the feasibility of other data search and/or production options.

The ZPIC shall obtain approval from the COR regarding requests started by the ZPIC that they subsequently anticipate will exceed that 40-hour level of effort. The ZPIC shall not exceed the 40-hour level of effort until it receives COR approval.

I. *Duplicate/Similar Requests for Information*

If the ZPIC receives duplicate or similar requests for information from OIG and DOJ, the ZPIC shall notify the requestors. If the requestors are not willing to share the information, the ZPIC shall ask the COR and IAG BFL for assistance.

J. *Reporting Requirements for the DOJ and OIG*

For each data request received from the DOJ and the OIG, the ZPIC 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*
- *The cost of furnishing a response to each request*
- *The date completed*

K. Law Enforcement *Requests for Medical Review*

The ZPIC shall not send document request letters or go onsite to providers/suppliers to obtain medical records solely at the direction of LE. However, if LE furnishes the medical records and requests the ZPIC to review and interpret medical records for them, the ZPIC shall require LE 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, what is the allegation, and what should the reviewer be looking for in the medical record);*
- *The volume of records furnished;*
- *The due date; and*
- *The format required for response.*

The ZPIC shall present the written request to the COR, and copy its IAG BFL prior to fulfilling the request. Each written request will be considered on a case-by-case basis to determine whether the ZPIC has resources to fulfill the request. If so, the request may be approved.

If LE requests the ZPIC to perform MR on all investigations the ZPIC initiates, the ZPIC shall perform MR if it deems it necessary, on a case-by-case basis. The ZPIC shall inform the COR and copy its IAG BFL of such requests by LE.

It is recommended that the MR Manager be included in the evaluation of the Request for MR to provide input as to:

- *The resources required;*
- *The resources available; and,*
- *Recommended revisions to the volume of records to be reviewed that will still provide a statistically and clinically significant sample to support the purpose or allegation in the request and provide for the best use of MR resources.*

L. ***Law Enforcement Requests for ZPIC Audits of Medicare Provider Cost Reports Relating to Fraud***

If LE requests the ZPIC to perform an audit of a Medicare provider's cost report for fraud, the ZPIC shall consult with the MAC to inquire if an audit of the cost report has already been performed. The ZPIC shall also consult with the COR and IAG BFL. The ZPIC shall provide its COR and copy its IAG BFL with the basis for the LE request and a detailed cost estimate to complete the audit. If the COR approves the audit, the ZPIC shall perform the audit within the time frame and cost agreed upon with LE.

M. Requests ***from Law Enforcement for Information Crossing Several ZPIC Zones***

If *a* ZPIC receives *a* request *from LE* for information *that crosses several* ZPIC *zones*, the ZPIC shall *contact its COR and IAG BFL. In the event that multiple zones are providing information in connection with the request, each ZPIC shall enter a separate entry into the FID as described in section 4.11.2.8 of this chapter. The COR and IAG BFL may assign a lead ZPIC to process these requests.*

4.4.1.1 - *Reserved for Future Use*

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

4.4.2 - Zone Program Integrity Contractor Coordination with Other Zone Program Integrity Contractors

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs.

The ZPIC shall coordinate with *ZPICs in* other *zones, as directed in the USOW and Task Order Statement of Works (SOWs).*

4.4.2.1 – Zone Program Integrity Contractor Coordination with Other Entities

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

The ZPIC shall establish and maintain formal and informal communication with state survey agencies, *the* OIG, *the* DOJ, s*tate* Medicaid *agency*, other Medicare contractors, other ZPICs, and other organizations as applicable to determine information that is available and that should be exchanged to enhance *program integrity* activities.

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

4.4.3 - *Reserved for Future Use*

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

4.5 - *Reserved for Future Use*

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

4.6.1 - Definition of a Complaint

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs and MACs.

A complaint is a statement, oral or written, alleging that a provider, supplier, or beneficiary received a Medicare *reimbursement or* benefit to which he or she is not entitled under current Medicare law, regulations, or policy. Included are allegations of misrepresentation and violations of Medicare requirements applicable to persons or entities that bill for covered items and services. Examples of complaints include *(this is not an exhaustive list)*:

- Allegations that items or services were not received*;*
- Allegations that items or services were not furnished as shown on the Explanation of Medicare Benefits (EOMB), Notice of Utilization (NOU), or Medicare Summary Notice (MSN), or that the services were not performed by the provider*/supplier* shown*;*
- Allegations that a provider*/supplier* is billing Medicare for a different item or service than *was* furnished*;*
- Allegations that a provider or supplier has billed both the beneficiary and Medicare for the same item or service*;*
- Allegations regarding waiver of co-payments or deductibles*;*
- Allegations that a supplier or provider has misrepresented itself as having an affiliation with an agency or department of the state, local, or federal government, whether expressed or implied*; and*
- *Allegations or inquiries from a b*eneficiary concerning payment for an item or service that, in his/her opinion far exceeds reasonable payment for the item or service that the beneficiary received (e.g., the supplier or physician has *"upcoded"* to receive higher payment).

The following are not examples of a fraud complaint *(this is not an exhaustive list)*:

- Complaints or inquiries regarding Medicare coverage policy;
- Complaints regarding the appeals process;
- Complaints over the status of a claim;
- Requests for an appeal or reconsideration; or
- Complaints concerning providers or suppliers (other than those complaints meeting the criteria established above) that are general in nature and are policy- or program-oriented.

Complaints alleging malpractice or poor quality of care may or may not involve a fraudulent situation. These *complaints* shall be reviewed and determined on a case-by-case basis. *The ZPIC shall r*efer complaints alleging poor quality of care to the Medicare/Medicaid survey and certification agencies and the QIO*s within two (2) business days*. *The ZPIC shall forward any medical records to the QIO upon receipt from the provider, when appropriate. Any complaints involving allegations of fraud shall be screened to determine if further investigation by the ZPIC is necessary.*

4.6.2 - Complaint Screening

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs, Beneficiary Contact Center (BCC), and MACs, as indicated.

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

A. Initial Screening – Beneficiary Contact Center

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

- Lab Tests - CSRs shall ask caller*s* if they recognize the referring physician. If they do, remind caller*s* that the referring physician may have ordered some lab work for them. The beneficiar*ies* usually do not have contact with the lab because specimens are sent to the lab by the referring physician office. (Tip: ask if they remember the doctor withdrawing blood or obtaining a tissue sample on their last visit).
- Anesthesia Services - CSRs shall check the beneficiary claims history for existing surgery or assistant surgeon services on the same date. If a surgery charge is on file, explain to the caller that anesthesia service is part of the surgery rendered on that day.
- Injections - CSRs shall check the beneficiary claim history for the injectable (name of medication) and the administration. Most of the time, *the* administration *of the injection* is not payable, *as it is a* bundled service *under* Part B only. There are very few exceptions to pay for the administration.
- Services for Spouse - If the beneficiar*ies* state that services were rendered to *their* spouse and the HICNs are the same, with a different suffix, the CSR shall initiate the adjustment and the overpayment process*es*.
- Billing Errors - If the beneficiar*ies* state that *they* already contacted *their* provider*/supplier* and the provider*/supplier* admitted there was a billing error *but a* check is still outstanding, the CSR shall follow the normal procedures for resolving this type of billing error.
- Services Performed on a Different Date - The beneficiar*ies* state that *a* service was rendered, but on a different date. *The CSR shall review the beneficiary claim history to determine if there are multiple dates billed for this service. If not, an adjustment to the claim may be required to record the proper date on the beneficiaries' file.*
- Incident to Services - Services may be performed by a nurse in a doctor's office as "incident to." These services are usually billed under the physician's provider*/supplier transaction access* number (P*TAN*) (e.g., blood pressure check, injections). These services may be billed under the minimal *e*valuation and *m*anagement codes.
- Billing Address vs. Practice Location Address - The CSR shall check the practice location address where services were rendered. Many times the Medicare Summary Notice will show the billing address, causing the beneficiaries to think the billing might be fraud.

The CSRs shall use proper probing questions and shall u*se* claim history files to determine if the *complaint or inquiry* needs to be referred for second-level screening.

Any provider*/supplier* inquiries regarding potential fraud*, waste,* and *abuse* shall be forwarded immediately to the second-level screening staff at the MAC for handling.

*I*mmediate advisements shall be forwarded immediately to the second-level screening staff at the MAC for handling. These advisements include inquiries or allegations by beneficiaries or providers*/suppliers* concerning kickbacks, bribes, or a crime by a *f*ederal employee (e.g., altering claims data or manipulating them to create preferential treatment to certain providers*/suppliers*; improper preferential treatment collecting overpayments; or embezzlement). *Indicators of contractor employee fraud shall be forwarded to the CMS Compliance Group.*

The OIG Hotline is an OIG managed system that accepts tips and complaints from all sources about potential fraud, waste, abuse in the Medicare, Medicaid and CHIP programs. Complaints and any relevant documents originating from the OIG Hotline will be sent to the responsible MAC by the OIG via e-mail. Each MAC shall establish a resource mailbox to receive complaints from the OIG. The MAC shall review these complaints and process them in accordance with all other applicable complaint screening processes unless otherwise noted. Complaints originating from the OIG Hotline that the MAC receives must include a Medicare number and/or complainant contact information. Upon receipt of an OIG Hotline complaint, the complaint shall be forwarded immediately to the second-level screening staff at the MAC for review and processing. If the complaint does not include a Medicare number and/or complainant contact information, the complaint shall be closed with no further action necessary.

B. Second-Level Screening – MAC

When the complaint *or* inquiry cannot be resolved by the CSR at the BCC, the issue shall be referred for more detailed screening, resolution, or referral, as appropriate, to the MAC. The second-level screening staff at the MAC shall only screen potential fraud*, waste,* and *abuse* complaints *or inquiries* with a paid amount of $100 or greater (includ*ing* the deductible as payment) or *three (*3*)* or more beneficiary complaints *or inquiries,* regardless of dollar amount*, about* the same provider*/supplier*. Each complaint *or inquiries* shall be tracked and retained for *one (*1*)* year. *Beneficiaries inquiring about complaints should be advised* that *they are being* tracked *and reviewed*. *The MAC shall perform a more in-depth review* if additional complaints *or inquiries* are received*. Complaints or inquiries that do not meet the threshold for second-level screening shall be closed.* The second-level screening staff at the MAC shall maintain a log of all potential fraud*, waste,* and *abuse complaints or* inquiries received from the initial screening staff. At a minimum, the log shall include the following information:

- Beneficiary name*;*
- *Provider/supplier* name*;*
- Beneficiary HIC*N;*
- Nature of the *i*nquiry*;*
- Date received from the initial screening staff*;*
- Date referral *was* sent to the ZPIC*;*
- Destination of the referral (i.e., name of the ZPIC)*;*
- Documentation that a *complaint or* inquiry received from the initial screening staff was not forwarded to the ZPIC and an explanation why (e.g., inquiry was misrouted or inquiry was a billing error that should not have been referred to the second-level screening staff)*; and*
- Date *complaint or* inquiry *was* closed.

The MAC staff shall call the beneficiary or the provider*/supplier*, check claims history, and check provider*/supplier* correspondence files for educational *or* warning letters or contact reports that relate to similar complaints *or inquiries*, to help determine whether or not there is a pattern of potential fraud*, waste,* and *abuse*. The MAC shall request and review certain documents, *such as itemized billing statements and other pertinent information,* as appropriate, from the provider*/supplier*. If the MAC is unable to make a determination on the nature of the complaint *or inquiry* (e.g., fraud*, waste,* and abuse, billing errors) based on the aforementioned contacts and documents, the MAC shall order medical records and limit the number of medical records ordered to only those required to make a determination.

If the medical records are not received within 45 business days, the claim(s) shall be denied. *I*f fraud is suspected when medical records are not received, these situations shall be referred to the ZPIC. The second-level screening staff shall only perform a billing and document review on medical records to verify that services were rendered. If fraud*, waste,* and abuse are suspected after performing the billing and document review, the medical record shall be forwarded to the ZPIC for clinician review. If the MAC staff determines that the complaint *or inquiry* is not a fraud and/or abuse issue, and if the staff discovers that the complaint *or*

inquiry has other issues (e.g., *MR*, enrollment, claims processing), it shall be referred to the appropriate department *and then closed*.

If the MAC second-level screening staff determines that the complaint *or inquiry* is a potential fraud*, waste,* and *abuse* situation, the second-level screening staff shall forward it to the ZPIC for further development within 45 business days of the date of receipt from the initial screening staff, or within 30 business days of receiving medical records and/or other documentation, whichever is later. The MAC shall refer immediate advisements received by beneficiaries or providers*/suppliers* and potential fraud*, waste,* or *abuse* complaints received by current or former provider*/supplier* employees immediately to the ZPIC for further development.

All OIG Hotline complaints *sent to the MAC by the OIG* shall be reviewed, determinations shall be made, and final action shall be taken within 45-business days after the complaints have been *received*, *even if additional documents have been requested but not yet received*. The MAC shall use the date contained in the *e-mail from the OIG* at the start of the 45-business day timeframe.

If the MAC requests additional documentation that is received after the 45-business day timeframe and the complaint is closed, the complaint shall be reopened but only if the additional information warrants further action or if the additional information would change the initial determination. The MAC has 30 business days from the date the complaint was reopened to take final action on the reopened complaint. If the MAC is the second contractor assigned to a complaint, the second contractor has 45 business days from the date the complaint is received to take final action on a complaint.

MACs that refer a complaint to the ZPIC shall notify the ZPIC via e-mail that a complaint is being referred as potentially fraudulent. The MAC shall develop a referral package (see below for what should be included in the referral package) for all complaints being referred to the ZPIC and shall send the complaint via a secure method such as e-mail or mail directly to the ZPIC.

Once the complaint has been referred to the ZPIC, the MAC *shall close the complaint in its internal tracking system. These referrals shall be done in accordance with the timeframes established above.*

If the MAC receives a complaint *from* the OIG that has been erroneously assigned to the MAC, the contractor shall transfer the erroneously assigned complaint to the appropriate MAC within 10 business days from the date it determined that the complaint was erroneously assigned.

To refer an erroneously assigned complaint to a MAC, the referring contractor shall send an e-mail containing all relevant complaint information and documents to the correct contractor notifying it that a complaint is being reassigned. Within 10 business days of receiving the e-mail, the receiving contractor shall review the complaint. Final action shall be taken in accordance with the timeframes established above.

The MAC shall refer complaints alleging fraud, waste, or abuse in the Medicaid program to the appropriate Program Integrity Unit (PIU) within the State Medicaid Agency (SMA) noted in Exhibit 47. Entities committing such fraud, waste, or abuse include but are not limited to: Medicaid providers; Medicaid recipients; Medicaid managed care organizations or waiver program contractors, their employees, agents or subcontractors. The MAC shall send the complaint information with any supporting documents to the appropriate PIU.
The MAC shall identify and refer complaints alleging fraud, waste, or abuse in the Medicare Part C or Part D programs to the MEDIC. This includes complaints that do not have a credible allegation of fraud.
The MAC shall identify and refer complaints alleging fraud, waste, or abuse involving the Federal Marketplace and State-Based Exchanges, insurance agents/brokers marketing Marketplace plans, and Marketplace consumers to the following email address: marketplaceintegrity@cms.hhs.gov, with a copy to the CORs. The MAC shall close the complaint in its internal tracking system. These referrals shall be done in accordance with the timeframes established above.

The MAC shall identify and refer complaints that do not allege fraud, waste, or abuse involving CMS programs (e.g., Social Security Administration, Health Resources and Services Administration, U.S. Department of Labor, and U.S. Department of Veterans Affairs) back to the OIG with a copy to the CORs. The MAC shall close the complaint in its internal tracking system. These referrals shall be done in accordance with the timeframes established above.
If the MAC receives duplicate complaints, they should be kept open and cross-reference the other complaint number(s). When the complaint is closed, monetary actions (if involved) shall only be claimed on the primary complaint, and the information updated on the duplicate complaint(s) should reference the same resolution of the primary complaint.

Complaints shall be forwarded to the ZPIC for further review under the circumstances *listed below* (this is *not an exhaustive list*):

- Claim forms may have been altered or up-coded to obtain a higher reimbursement amount;
- *Documentation appears to indicate that the provider/supplier has* attempted to obtain duplicate reimbursement (e.g., billing both Medicare and the beneficiary for the same service or billing both Medicare and another insurer in an attempt to be paid twice). This *apparent double-billing* does not include routine assignment violations. An example for referral might be that a provider*/supplier* has submitted a claim to Medicare, and then in *two (*2*) business* days resubmits the same claim in an attempt to bypass the duplicate edits and gain double payment. *A referral shall be made in instances where the provider/supplier has done the above repeatedly, indicating a potential pattern;*
- Potential misrepresentation with respect to the nature of the services rendered, charges for the services rendered, identity of the person receiving the services, identity of persons or doctor providing the services, dates of the services, etc;
- Alleged submission*s* of claims for non-covered services are misrepresented as covered services, excluding demand bills and those with Advanced Beneficiary Notices (ABNs);
- Claims involving potential collusion between a provider*/supplier* and a beneficiary resulting in higher costs or charges to the Medicare program;
- Alleged use of another person's Medicare number to obtain medical care;
- Alleged alteration of claim history records to generate inappropriate payments;
- Alleged use of the adjustment payment process to generate inappropriate payments; *or*
- Any other instance that is likely to indicate a potential fraud*, waste,* and abuse *situation*.

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

When the above situations occur *requiring that the complaint be referred to the ZPIC for review,* the MAC shall prepare a referral package that includes, at a minimum, the following:

- Provider*/supplier* name, provider*/supplier* number, and address.
- Type of provider*/supplier* involved in the allegation and the perpetrator, if an employee of the provider*/supplier*.
- Type of service involved in the allegation.
- Place of service.
- Nature of the allegation(s).
- Timeframe of the allegation(s).
- Narration of the steps taken and results found during the MAC's screening process (discussion of beneficiary contact, if applicable, information determined from reviewing internal data, etc.).
- Date of service, procedure code(s).

- Beneficiary name, beneficiary HICN, telephone number.
- Name and telephone number of the MAC employee who received the complaint.

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

When a provider*/supplier* inquiry or complaint of potential fraud or *IA* is received, the second-level screening staff *shall* not perform any screening but *shall* prepare a referral package *within two business days of when this inquiry or IA was received,* and send it to the ZPIC *during the same timeframe*. The referral package shall consist of the following information:

- Provider*/supplier* name and address.
- Type of provider*/supplier* involved in the allegation and the perpetrator, if an employee of a provider*/supplier*.
- Type of service involved in the allegation.
- Relationship to the provider*/supplier* (e.g., employee or another provider*/supplier*).
- Place of service.
- Nature of the allegation(s).
- Timeframe of the allegation(s).
- Date of service, procedure code(s).
- Name and telephone number of the MAC employee who received the complaint.

The MAC shall maintain a copy of all referral packages.

4.6.2.1 – Zone Program Integrity Contractor Responsibilities

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs and MACs, as indicated.

When the complaint is received from the MAC screening staff, the ZPIC shall further screen the complaint, resolve the complaint, or make referrals as needed to the appropriate entity.

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

If the ZPIC staff determines, after screening the complaint, that it is not a potential fraud, waste, and/or abuse issue, but involves other issues (e.g., MR, enrollment, claims processing), the complaint shall be referred to the MAC area responsible for second-level screening. The MAC second-level screening staff shall track the complaints returned by the ZPIC. However, the ZPIC shall send an acknowledgement to the complainant, indicating that a referral is being made, if applicable, to the appropriate MAC unit for further action.

The ZPIC shall track complaints referred by the MAC second-level screening area in the ZPIC's internal tracking system.

The ZPIC shall send the complainant a resolution letter within seven (7) calendar days of resolving the complaint investigation.

4.6.3 – *Screening Leads*

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs.

Screening is the initial step in the review of a lead (described in section 4.2.2 of this chapter) to determine the need to perform further investigation based on the potential for fraud, waste, or abuse. Screening shall be completed within 21 calendar days after receipt of the lead.

The receipt date of the lead is generally determined by the date the ZPIC receives a complaint. If the lead resulted from data analysis conducted by the ZPIC, the receipt of the lead shall be the date the lead was referred from the ZPIC data analysis department to its investigation or screening unit. For a new lead that is identified from an active or current ZPIC investigation, the receipt of the lead shall be the date the new lead was identified by the ZPIC investigator.

Note: If criteria for an IA are met during evaluation of the lead, the ZPIC shall forward the IA to LE and continue to screen the lead, if deemed appropriate.

Activities that the ZPIC may perform in relation to the screening process include, but are not limited to:

- *Verification of provider's enrollment status;*
- *Data analysis;*
- *Contact with the complainant, when the lead source is a complaint;*
- *Beneficiary interviews;*
- *Referring/ordering physician interviews if there is no indication that the physician(s) are involved in the scheme related to the lead; and*
- *Site verification to validate the provider's/supplier's practice location.*

Any screening activities shall not involve contact with the subject provider/supplier or implementation of any administrative actions (i.e., post-payment reviews, prepayment reviews/edits, payment suspension, and revocation). However, if the lead is based solely on a potential assignment violation issue, the ZPIC may contact the provider directly to resolve only the assignment violation issue. If there are circumstances noted in FID that would raise additional concerns, the ZPIC shall contact its COR and IAG BFL for further guidance. If the lead involves potential patient harm, the ZPIC shall immediately notify CMS within two (2) business days.
After completing its screening, the ZPIC shall close the lead if it does not appear to be related to fraud, waste, or abuse. Prior to closing the lead, the ZPIC shall take any appropriate actions (i.e., referrals to the MAC, RA, state, or QIO). For example, if a lead does not appear to be related to potential fraud, waste, or abuse but the lead needs to be referred to the MAC, the date that the ZPIC refers the information to the MAC is the last day of the screening.

At a minimum, the ZPIC shall document the following information in its case file:

- The date the *lead* was received *and closed;*
- *Lead source (e.g., beneficiary, MAC, provider/supplier);*
- *Record the name and telephone number of the individual (or organization), if applicable, that provided the information concerning the alleged fraud or abuse;*
- *Indicate* the *provider's/supplier's name, address, and ID number;*
- *Start and end date of the screening;*
- *Description of the actions/activities performed;*

- *Start and end date of each action/activity;*
- *A* brief description of the action taken to close *the lead (e.g.*, *r*eviewed records and substantiated amounts billed*). E*nsure that sufficient information is provided to understand the reason for the closeout;
- The number of *leads* received to date *regarding* this provider*/supplier*, including the present *lead*. This information is useful in identifying providers*/suppliers* that are involved in an undue number of complaints; *and*
- *Any documentation associated with the ZPIC's activities (i.e., referrals to other entities).*

Additionally, if the screening process exceeds 21 calendar days, the ZPIC shall document the reasons, circumstances, dates, and actions associated with the delay to its COR and IAG BFL within its monthly reporting in CMS ARTS.

4.6.4 - Vetting Leads with CMS

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

All leads and any new subjects that the ZPIC determines warrant further investigation shall be vetted through CMS for approval before transitioning to an investigation. The ZPIC shall submit the lead to CMS within two (2) business days of the ZPIC determining that the lead should be transitioned into an investigation. For the submission to CMS, the ZPIC shall use the designated CMS Vetting Form, which shall include, at a minimum, NPI, name, and practice location.

The ZPIC shall only open investigations on leads that are approved by CMS. If the ZPIC is instructed by CMS to close the lead without further action, the ZPIC shall do so within two (2) business days. If the screening results in a new investigation or becomes part of an existing investigation, the aforementioned screening information shall become part of the investigation file. If, during the course of a ZPIC investigation, it is determined that additional NPIs should be incorporated into the ongoing investigation, the ZPIC shall vet each additional NPI with CMS utilizing the approved CMS process described above before implementing any investigative actions (noted in section 4.7 of this chapter) on the additional NPIs. For any new investigations, the ZPIC shall complete the appropriate updates in the FID within seven (7) calendar days.

4.7 - Investigations

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

This section applies to ZPICs.

An investigation is the *expanded* analysis performed on leads *once such lead is vetted and approved by CMS to be opened as an investigation. The ZPIC shall focus its investigation* in an effort to *establish the facts and the magnitude of the alleged fraud, waste, or abuse and take any appropriate action to protect Medicare Trust Fund dollars*.

Activities that the ZPIC may perform in relation to the investigative process include, but are not limited to:

- *Screening activities noted in section 4.6.3 of this chapter;*
- *Contact with the provider via telephone or on-site visit;*
- *Medical record requests and reviews (as defined in PIM, chapter 3);*
- *Implementation of auto-denial edits; and*
- *Administrative actions (as defined in PIM chapters 3, 8, and 15).*

For any investigative activities that require preapproval by CMS (i.e., payment suspensions, and revocations), the ZPIC shall submit those requests to CMS for approval with a copy to its COR and BFLs for approval when initiating those actions.

Prioritization of the investigation workload is critical to ensure that the resources available are devoted primarily to high-priority investigations.

The ZPIC shall maintain files on all investigations. The files shall be organized by provider or supplier and shall contain all pertinent documents *including, but not limited to, the* original referral or complaint, investigative findings, reports of telephone contacts, warning letters, documented discussions, *documented results of any investigative activities,* any data analysis or analytical work involving the potential subject or target of the investigation, and decision memoranda regarding final disposition of the investigation (refer to section 4.2.2.4.2 of this chapter for information concerning the retention of these documents).

Under the terms of their contract, the ZPICs shall investigate potential fraud*, waste, or abuse* on the part of providers, suppliers, and other entities that receive reimbursement under the Medicare program for services rendered to beneficiaries. The ZPICs shall refer potential fraud cases to *LE*, as appropriate, and provide support for these cases. In addition, the ZPICs may provide data and other information related to potential fraud cases initiated by *LE* when the cases involve entities or individuals *that* receive reimbursement under the Medicare program for services rendered to beneficiaries.

For those investigations that are national in scope, CMS will designate a lead ZPIC, if appropriate, to facilitate activities across the zones.

4.7.1 – Conducting Investigations

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

The ZPIC shall*, unless otherwise advised by CMS*, use one or more of the following investigative methods (*this is not an exhaustive list.*)*:*

- Perform validation checks of physician licensure;
- Perform data analysis (ZPICs shall follow PIM*,* chapter 2);
- Initiate other analysis enhancements to authenticate proper payments;
- Interview 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 potentially inappropriate claims or if this was a one-time occurrence;
- Look for past contacts by the ZPIC or the *MAC* 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. Coordinate with MR and audit staff, as appropriate;
- Review telephone calls or *mail* written questionnaires to physicians, confirming the need for home health services or DMEPOS;
- *Perform provider/supplier onsite visits and/or provider/supplier interviews;*
- Review a small sample of claims submitted within recent months. Depending on the nature of the problem, the ZPIC may need to request medical documentation or other evidence that would validate or cast doubt on the validity of the claims; *and*
- *Analyze and* compile *relevant* documentation (e.g., medical records or cost reports).

After reviewing the provider's*/supplier's* background, specialty*,* and profile, *the* ZPIC decide*s* whether the situation *involves* potential fraud*, waste, or abuse*, or may be more accurately categorized as a billing error. For example, records *might* indicate that a physician has billed, in some instances, both Medicare and the beneficiary for the same service. Upon review, *the ZPIC may* determine that, rather than attempting to be paid twice for the same service, the physician made an error in his/her billing methodology. Therefore, this *error* would be considered a determination of *incorrect* billing, rather than *potential* fraud*, waste, or abuse*

involving intentional duplicate billing. *If the ZPIC determines that an overpayment exists solely on data analysis, the ZPIC shall obtain COR and IAG BFL approval prior to initiating the overpayment.*

4.7.2 – Closing Investigations

(Rev. 675, Issued: 09-09-16, Effective: 12- 12 -16, Implementation: 12-12-16)

An investigation shall be closed if it is referred to *LE* (i.e., it is referred to OIG, DOJ, FBI, or AUSA) *and there are no pending administrative actions. In addition, an investigation may be closed due to the following circumstances:*

- *When no further action is warranted by the ZPIC and the matter* is referred back to the MAC or to another *CMS contractor for further review;*,
- *I*f it is closed with administrative action*(s)*;
- *If the potential fraud is not substantiated; and/or*
- *If CMS declined a requested administrative action.*

Medicare Program Integrity Manual
Exhibits

Table of Contents
(Rev.)

Exhibit 47 – Program Integrity Unit Contacts within the State Medicaid Agency

State	POC	Phone	POC E-mail Address
Alabama	*Jacqueline Thomas*	*(334) 242-5318*	*jacqueline.thomas@medicaid.alabama.gov*
Alaska	*Doug Jones*	*(907) 269-0361*	*doug.jones@alaska.gov*
American Samoa	*Sandra King Young*	*(684) 633-4818*	*sandrakingyoung@gmail.com*
Arizona	*Sharon Ormsby*	*(602) 417-4535*	*Sharon.Ormsby@azahcccs.gov*
Arkansas	*Elizabeth Thomas Smith*	*(501) 683-6404*	*Elizabeth.Smith@governor.arkansas.gov*
California	*Bruce Lim*	*(916) 440-7552*	*bruce.lim@dhcs.ca.gov*
Colorado	*Katherine Quinby*	*(303) 866-4940*	*katherine.quinby@state.co.us*
Connecticut	*John McCormick*	*(860) 424-5920*	*john.mccormick@ct.gov*
Delaware	*Linda Murphy*	*(302) 255-9801*	*linda.murphy@state.de.us*
District of Columbia	*Donald Shearer*	*(202) 698-2007*	*Donald.Shearer@dc.gov*
Florida	*Jennifer Ellingsen* *Fred Becknell*	*(850) 412-3977*	*Jennifer.Ellinsen@myflorida.com* *Fred.Becknell@myflorida.com*
Georgia	*Terri Kight*	*(404) 463-7437*	*tkight@dch.ga.gov*
Guam	*Theresa Arcangel (also SMD)*	*671-735-7282*	*theresa.arcangel@dphss.guam.gov*
Hawaii	*Shelley Siegman (Acting)*	*(808) 692-8095*	*ssiegman@medicaid.dhs.state.hi.us*
Idaho	*Lori Stiles*	*(208) 334-0653*	*stilesl@dhw.idaho.gov*
Illinois	*Bradley Hart*	*(217) 524-5105*	*bradley.hart@illinois.gov*
Indiana	*John McCullough*	*317-234-2129*	*John.Mccullough@fssa.IN.gov*
Iowa	*Rocco Russo*	*(515) 256-4632*	*rrusso@dhs.state.ia.us*
Kansas	*Krista Engel*	*(785) 296-7286*	*KEngel@kdheks.gov*
Kentucky	*Veronica Cecil*	*(502) 564-5472 ext 2253*	*Veronica.Cecil@Ky.gov*
Louisiana	*Ruth Kennedy* *Jen Steele (Deputy)*	*(225) 342-3032*	*Ruth.Kennedy@la.gov* *Jen.Steele@la.gov*
Maine	*Herb F. Downs*	*(207) 287-2778*	*Herb.F.downs@maine.gov*
Maryland	*Susan Steinberg*	*(410) 767-6039*	*Susan.Steinberg@maryland.gov*
Massachusetts	*Joan Senatore*	*(617) 348-5380*	*joan.senatore@state.ma.us*
Michigan	*MI Corp Email Account*		*dch-oig@michigan.gov*
Minnesota	*Jennifer Hasbargen*	*(651) 431-4356*	*jennifer.hasbargen@state.mn.us*
Mississippi	*Otis Washington, Jr.*	*(601) 576-4135*	*Otis.Washington@medicaid.ms.gov*
Missouri	*Jessica Dresner*	*(573) 751-3399*	*Jessica.Dresner@dss.mo.gov*
Montana	*Michelle Truax*	*(406) 444-4120*	*MTruax@mt.gov*
Nebraska	*Anne Harvey*	*(402) 471-1718*	*anne.harvey@nebraska.gov*
Nevada	*Tammy Moffitt*	*(775) 684-3623*	*Tammy.Moffitt@dhcfp.nv.gov*

State	POC	Phone	POC E-mail Address
New Hampshire	*Sherry Bozoian*	*(603) 271-8029*	*sbozoian@dhhs.state.nh.us*
New Jersey	*Elissa Smith*	*(609) 292-4350*	*Elissa.Smith@osc.state.nj.us*
New Mexico	*Everet Apodaca*	*(505) 827-3135*	*everet.apodaca@state.nm.us*
New York	*Corp. Email Account*		*Bmfa@omig.ny.gov*
North Carolina	*Rob Kindsvatter*	*(919) 814-0123*	*Rob.kindsvatter@dhhs.nc.gov*
North Dakota	*Dawn Mock*	*(701) 328-1895*	*dmock@nd.gov*
Northern Mariana Islands	*Helen Sablan*	*670-664-4884*	*chcmc@pticom.com*
Ohio	*Rachel Jones*	*N/A*	*Rachel.jones@medicaid.ohio.gov*
Oklahoma	*Kelly Shropshire*	*(405) 522-7131*	*Kelly.Shropshire@okhca.org*
Oregon	*Charles Hibner*	*(503) 378-8113*	*charles.hibner@state.or.us*
Pennsylvania	*Clint Eisenhower (Acting)*	*(717) 214-1942*	*ceisenhowe@pa.gov*
Puerto Rico	*Luz Cruz-Romero* *Ricardo Rivera Cardona*	*(787) 765-4044* *(787) 474-3300 ext. 3003*	*luz.cruz@salud.pr.gov* *raivera@asespr.org*
Rhode Island	*Bruce McIntyre*	*(401) 462-0613*	*bruce.mcintyre@ohhs.ri.gov*
South Carolina	*Betty Jane (BJ) Church*	*(803) 898-2678*	*church@scdhhs.gov*
South Dakota	*Lori Lawson (Interim)*	*(605) 773-3495*	*Lori.Lawson@state.sd.us*
Tennessee	*Dennis J Garvey*	*(615) 507-6696*	*Dennis.J.Garvey@tn.gov*
Texas	*Stuart Bowen, Jr.*	*(512) 491-2051*	*Stuart.bowen@hhsc.state.tx.us*
Utah	*Noleen Warrick*	*(801) 538-6455*	*noleenwarrick@utah.gov*
Vermont	*Ron Clark (ret. 2/20/15)* *Leanne Miles (eff. 2/20/15)*	*(802) 879-5652* *(802) 879-5964*	*ron.clark@state.vt.us* *Leanne.miles@state.vt.us*
Virgin Islands	*Renee Joseph-Rhymer*	*(340) 774-0930*	*Renee.JosephRhymer@dhs.vi.gov*
Virginia	*Louis Elie*	*(804) 786-5590*	*louis.elie@dmas.virginia.gov*
Washington	*Cathie Ott (Acting)*	*(360) 725-2116*	*cathie.ott@hca.wa.gov*
West Virginia	*Tammy G. Hypes*	*(304) 356-4885*	*Tammy.G.Hypes@wv.gov*
Wisconsin	*Alan White*	*(608) 266-7436*	*alan.white@dhs.wisconsin.gov*
Wyoming	*Mark Gaskill*	*(307) 777-2054*	*Mark.gaskill@wyo.gov*