CMS Manual System	Department of Health & Human Services (DHHS)
Pub 100-08 Medicare Program Integrity	Centers for Medicare & Medicaid Services (CMS)
Transmittal 851	**Date: December 14, 2018**
	Change Request 10591

Transmittal 827, dated September 21, 2018, is being rescinded and replaced by Transmittal 851, dated December 14, 2018, to add a revision to subsection 4.6.2.3.B. (Screening of OIG Hotline Referrals) of chapter 4. Part B Screening of OIG Hotline Referrals allows ten (10) business days to prepare a referral package when a complaint meeting the criteria of an IA or potential fraud, waste or abuse is received. The current manual instructions in this section only allows for two (2) business days. All other information remains the same.

SUBJECT: Updates to Chapter 4 of Publication (Pub.) 100-08

I. SUMMARY OF CHANGES: The purpose of this Change Request (CR) is to update various sections within chapter 4 of Pub. 100-08.

EFFECTIVE DATE: October 22, 2018
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: October 22, 2018

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	4/4.1/Introduction
R	4/4.2/Medicare Program Integrity
R	4/4.2/4.2.1/Examples of Medicare Fraud
R	4/4.2/4.2.2/Unified Program Integrity Contractor
R	4/4.2/4.2.2/4.2.2.1/Organizational Requirements
R	4/4.2/4.2.2/4.2.2.2/Liability of Unified Program Integrity Contractor Employees
R	4/4.2/4.2.2/4.2.2.3/Anti-Fraud Training
R	4/4.2/4.2.2/4.2.2.3/4.2.2.3.1/Training for Law Enforcement Organizations
R	4/4.2/4.2.2/4.2.2.4/Procedural Requirements
R	4/4.2/4.2.2/4.2.2.4/4.2.2.4.1/Maintain Controlled Filing System and Documentation
R	4/4.2/4.2.2/4.2.2.4/4.2.2.4.2/File/Document Retention
R	4/4.2/4.2.2/4.2.2.6/Program Integrity Security Requirements
R	4/4.2/4.2.3/Durable Medical Equipment Medicare Administrative Contractor Fraud Functions
R	4/4.3/Medical Review for Program Integrity Purposes
R	4/4.4/4.4.1/Requests for Information From Outside Organizations
R	4/4.4/4.4.2/Unified Program Integrity Contractor Coordination with Other Unified Program Integrity Contractors
R	4/4.4/4.4.2/4.4.2.1/Unified Program Integrity Contractor Coordination with Other Entities
R	4/4.4/4.6/4.6.1/Definition of a Complaint
R	4/4.6/4.6.2/Complaint Screening
R	4/4.6/4.6.2/4.6.2.1/Contact Center Operations
N	4/4.6/4.6.2/4.6.2.2/OIG Hotline
N	4/4.6/4.6.2/4.6.2.3/MAC Complaint Screening
N	4/4.6/4.6.2/4.6.2.4/Referrals to the UPIC
N	4/4.6/4.6.2/4.6.2.5/Unified Program Integrity Contractor Responsibilities
R	4/4.6/4.6.3/Screening Leads
R	4/4.6/4.6.4/Vetting Leads with CMS
R	4/4.7/Investigations
R	4/4.7/4.7.1/Conducting Investigations
R	4/4.7/4.7.2/Closing Investigations
R	4/4.8/Disposition of Cases Referred to Law Enforcement

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
R	4/4.8/4.8.1/Reversed Denials by Administrative Law Judges on Open Cases
R	4/4.8/4.8.2/Production of Medical Records and Documentation for an Appeals Case File
R	4/4.9/Incentive Reward Program
R	4/4.9/4.9.1/UPIC Responsibilities for the Incentive Reward Program
R	4/4.9/4.9.2/Guidelines for Processing Incoming Complaints
R	4/4.9/4.9.3/Guidelines for Incentive Reward Program Complaint Tracking
R	4/4.9/4.9.4/Excluded Individuals
R	4/4.9/4.9.6/Unified Program Integrity Contractor Responsibilities
R	4/4.9/4.9.6/4.9.6.1/Guidelines for Processing Incoming Complaints
R	4/4.9/4.9.6/4.9.6.2/Guidelines for Incentive Reward Program Complaint Tracking
R	4/4.9/4.9.6/4.9.6.3/Overpayment Recovery
R	4/4.9/4.9.6/4.9.6.4/Eligibility Notification
R	4/4.9/4.9.6/4.9.6.5/Incentive Reward Payment
R	4/4.9/4.9.6/4.9.6.6/Reward Payment Audit Trail
R	4/4.9/4.9.7/CMS Incentive Reward Winframe Database
R	4/4.9/4.9.8/Updating the Incentive Reward Database
R	4/4.10/Fraud Alerts
R	4/4.11/4.11.2/4.11.2.3/Initial Entry Requirements for DMEPOS Payment Suspensions
R	4/4.13/Administrative Relief from Program Integrity Review in the Presence of a Disaster
R	4/4.14/Provider/Supplier Contacts by the UPIC
N	4/4.15/Reserved for Future Use
R	4/4.16/MAC and UPIC Coordination on Voluntary Refunds
R	4/4.18/4.18.1/Referral of Cases to the OIG/OI
R	4/4.18/4.18.1/4.18.1.2/Immediate Advisements to the OIG/OI
R	4/4.18/4.18.1/4.18.1.3/Payment Suspension
R	4/4.18/4.18.1/4.18.1.4/OIG/OI Referral and Summary Report
D	4/4.18/4.18.1/4.18.1.3/4.18.1.3.1/Suspension
D	4/4.18/4.18.1/4.18.1.3/4.18.1.3.2/Denial of Payments for Cases Referred to and Accepted by OIG/OI
D	4/4.18/4.18.1/4.18.1.3/4.18.1.3.3/Recoupment of Overpayments

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
R	4/4.18/4.18.1/4.18.1.4/OIG/OI Referral and Summary Report
R	4/4.18/4.18.1/4.18.1.5/Referral to Other Law Enforcement Agencies
R	4/4.18/4.18.1/4.18.1.5/4.18.1.5.1/Continue to Monitor Provider and Document Case File
R	4/4.18/4.18.1/4.18.1.5/4.18.1.5.2/Take Administrative Action on Cases Referred to and Refused by OIG/OI
R	4/4.18/4.18.1/4.18.1.5/4.18.1.5.3/Refer to Other Law Enforcement Agencies
R	4/4.18/4.18.2/Referral to State Agencies or Other Organizations
R	4/4.18/4.18.3/UPICs and QIOs
N	4/4.18/4.18.4/Referral of Cases to the MAC
R	4/4.19/4.19.1/The Unified Program Integrity Contractor’s and Medicare Administrative Contractor’s Role
R	4/4.19/4.19.2/Authority to Exclude Practitioners, Providers, and Suppliers of Services
R	4/4.19/4.19.2/4.19.2.2/Identification of Potential Exclusion Cases
R	4/4.19/4.19.2/4.19.2.3/Development of Potential Exclusion Cases
R	4/4.19/4.19.2/4.19.2.4/Contents of Sanction Recommendation
R	4/4.19/4.19.2/4.19.2.6/4.19.2.6.1/Denial of Payment to Employer of Excluded Physician
R	4/4.19/4.19.4/Reinstatements
R	4/4.19/4.19.4/4.19.4.1/Monthly Notification of Sanction Actions
R	4/4.20/4.20.1/4.20.1.2/Purpose
R	4/4.20/4.20.1/4.20.1.4/Administrative Actions
R	4/4.20/4.20.3/4.20.3.1/Referral Process to CMS
R	4/4.20/4.20.3/4.20.3.2/Referrals to OIG
R	4/4.20/4.20.4/CMS Generic Civil Monetary Penalties Case Contents
R	4/4.20/4.20.5/4.20.5.1/Beneficiary Right to Itemized Statement
R	4/4.21/Monitor Compliance
R	4/4.21/4.21.1/Resumption of Payment to a Provider - Continued Surveillance After Detection of Fraud
R	4/4.22/Discounts, Rebates, and Other Reductions in Price
R	4/4.22/4.22.1/4.22.1.1/Marketing to Medicare Beneficiaries
R	4/4.22/4.22.2/Cost-Based Payment (Intermediary and MAC Processing of Part A Claims): Necessary Factors for Protected Discounts

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
R	4/4.22/4.22.3/Charge-Based Payment (MAC Processing of Part B Claims): Necessary Factors for Protected Discounts
R	4/4.22/4.22.4/Risk-Based Provider Payment: Necessary Factors for Protected Discounts
R	4/4.23/Identity Theft – Physicians
R	4/4.28/Joint Operating Agreement
R	4/4.31/Vulnerabilities
R	4/4.33/UPIC Coordination with Other Contractors Related to the RAC Data Warehouse
R	4/4.34/Suppression and/or Exclusion – Examples

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: 851	Date: December 14, 2018	Change Request: 10591

Transmittal 827, dated September 21, 2018, is being rescinded and replaced by Transmittal 851, dated December 14, 2018, to add a revision to subsection 4.6.2.3.B. (Screening of OIG Hotline Referrals) of chapter 4. Part B Screening of OIG Hotline Referrals allows ten (10) business days to prepare a referral package when a complaint meeting the criteria of an IA or potential fraud, waste or abuse is received. The current manual instructions in this section only allows for two (2) business days. All other information remains the same.

SUBJECT: Updates to Chapter 4 of Publication (Pub.) 100-08

EFFECTIVE DATE: October 22, 2018
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: October 22, 2018

I. GENERAL INFORMATION

A. Background: The Centers for Medicare and Medicaid Services (CMS) is making revisions to Chapter 4 of Pub. 100-08 based on updates to Unified Program Integrity Contractor (UPIC) and Medicare Administrative Contractor (MAC) processes and 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	Shared-System Maintainers				Other
		A	B	HHH	MAC	FISS	MCS	VMS	CWF	
10591.1	The focus of the UPICs and MACs shall be to ensure compliance with Medicare regulations, refer suspected fraud and abuse to our Law Enforcement partners, and/or revocation of providers that are non-compliant with Medicare regulation and policies.	X	X	X	X					UPICs
10591.2	When the UPIC makes the determination that a matter is not potential fraud, waste, and/or abuse, the UPIC shall close the matter, or de-escalate the matter to the appropriate unit at the MAC, Quality	X	X	X	X					UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	Improvement Organization, or other entity, when appropriate.									
10591.3	The UPIC shall follow the requirements in its UPIC Statement Of Work for prioritizing leads.									UPICs
10591.4	The UPIC shall be expected to follow the current vetting process and the requirements of Chapter 4 of Pub. 100-08, §4.41 G, K, and L.									UPICs
10591.4.1	The UPIC shall consult with the Business Function Leads (BFL) and Contractor Officer Representative (COR) if questions arise about complying with law enforcement requests for medical records, conducting interviews, or refraining from specific administrative actions.									UPICs
10591.5	The UPIC shall maintain its workload in the Unified Case Management (UCM) system, unless otherwise directed by CMS.									UPICs
10591.6	For UPICs in transition, all existing electronic files for all years shall be transferred into UCM. Any hard copy files (that do not need to be retained indefinitely) older than 10 years shall be destroyed.									UPICs
10591.6.1	For UPICs in operation, all paper/hard copy files older than 10 years (that do not need to be retained indefinitely) shall be									UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	destroyed.									
10591.6.2	The UPICs shall scan as an electronic file any hard copy files older than 10 years that are part of a current investigation or litigation.									UPICs
10591.6.2.1	The UPICs shall destroy the hard copy files after certification that they have been properly scanned.									UPICs
10591.6.3	All scanned/electronic copies shall be transferred to the UCM.									UPICs
10591.7	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 or Recovery Audit Contractor (RAC) personnel should discuss potential referral of the matter to the UPIC.	X	X	X	X					RAC, UPICs
10591.7.1	If the UPIC agrees that there is potential fraud, waste, and/or abuse, the MAC or RAC personnel shall escalate and refer the matter to the UPIC.	X	X	X	X					RAC, UPICs
10591.7.2	Provider/supplier documentation that shows a pattern of repeated misconduct or conduct that is clearly abusive or potentially fraudulent, despite provider/supplier	X	X	X	X					RAC, UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	education and direct contact with the provider/supplier to explain identified errors, shall be referred to the UPIC.									
10591.8	The UPICs shall identify procedures that may make Medicare and Medicaid vulnerable to questionable billing or improper practices and take appropriate action.									UPICs
10591.9	The UPIC and MAC shall have the option to add language to their Joint Operating Agreement (JOA) that allows for a shorter timeframe for the MAC to furnish the requested information (e.g., 48 hours or 72 hours), as instructed in section 4.4.1, Chapter 4, Pub. 100-08.	X	X	X	X					UPICs
10591.10	The Contact Center Operations (CCO) Customer Service Representatives (CSR) shall use proper probing questions and shall use claim history files to determine if the complaint or inquiry needs to be referred to the MAC for additional screening.									UPICs
10591.10.1	The CCO CSRs shall immediately refer any provider/supplier inquiries regarding potential fraud, waste, and abuse to the MAC for handling and screening.									UPICs
10591.10.2	The CCO CSRs shall immediately refer									UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	Immediate advisements to the MAC for handling and screening.									
10591.11	Should the UPIC receive an Office of the Inspector General (OIG) Hotline complaint directly from the OIG, the UPIC shall proceed with the necessary screening, vetting, and investigative steps, as described in sections 4.6.3, 4.6.4, and 4.6.5, Chapter 4, Pub. 100-08.									UPICs
10591.12	The MAC shall follow the complaint screening process, as described in section 4.6.2.3, Chapter 4, Pub. 100-08.	X	X	X	X					
10591.13	The MAC and UPIC shall follow the complaint referral process, as described in section 4.6.2.4, Chapter 8, Pub. 100-08.	X	X	X	X					UPICs
10591.14	The UPIC shall vet all applicable National Provider Identifiers and Provider Identifiers associated with the provider or supplier's tax-identification number, when initially vetting the lead with CMS.									UPICs
10591.14.1	Once the lead is approved by CMS, the UPIC shall notate the date the lead was initially vetted and approved by CMS in the Fraud Investigation Database/UCM.									UPICs
10591.14.2	If multiple contractors become involved with the investigation, the UPIC									UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	that initially vetted the lead with CMS shall become the lead contractor, unless otherwise specified by CMS.									
10591.14.3	The lead contractor shall notify all applicable contractors of the date the lead was vetted and approved by CMS for investigation.									UPICs
10591.14.4	The other participating contractors shall also notate the date the lead was initially vetted and approved by CMS in their applicable case tracking system(s).									UPICs
10591.15	For investigations that the providers/suppliers are subject to prior authorization by the MAC, the UPIC should request the MAC to release the prior authorization requirement prior to pursuing the investigation further.	X	X	X	X					UPICs
10591.16	In instances where a medical review 100 percent denial is due to lack of documentation, the UPIC shall consult with its COR and BFL prior to initiation of overpayment notification actions, including any coordination with the MAC or notice to the provider/supplier.	X	X	X	X					UPICs
10591.16.1	If approved, the UPIC shall coordinate the recovery actions with the MAC, who would be responsible for									UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	processing the overpayment demand to the provider or supplier.									
10591.16.2	If denied, the UPIC shall follow the instructions provided by its COR and Investigations and Audits Group (IAG) BFL.									UPICs
10591.17	Once Fraud Alert information is disseminated, the UPIC shall have the option to send any questions related to the Fraud Alert to the COR and IAG BFL.									UPICs
10591.18	The lead-UPIC identified during the initial vetting process shall continue to be the lead-UPIC for a durable medical equipment, prosthetics, orthotics and supplies payment suspension, unless otherwise directed by CMS.									UPICs
10591.19	The UPICs shall include the statement described in section 4.14E, Chapter 4, Pub. 100-08, in all post payment correspondence that include an error rate, and if applicable, other communications that identify non-compliant billings and inform the provider/supplier of their non-compliance with Medicare requirements.									UPICs
10591.20	When a case has been rejected by law enforcement, UPICs shall consult with the COR, BFL, or Suspension subject matter expert concerning the imposition									UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	of suspension.									
10591.21	The UPICs shall follow the Referral of Cases to the MAC process, as described in section 4.18.4, Chapter 4, Pub. 100-08.									UPICs
10591.22	A UPIC that learns of a questionable discount program shall contact its IAG BFL to determine the course of action, when needed.									UPICs
10591.23	In instances of potential physician identity theft, if appropriate, the UPIC shall provide the COR and IAG BFL the information as described in section 4.23, Chapter 4, Pub. 100-08.									UPICs
10591.24	To account for instances where the UPIC is in need of requested information from the MAC in a shorter timeframe than 30 calendar days, the UPIC and MAC shall have the option to add language to their JOA that allows for a shorter timeframe for the MAC to furnish the requested information (e.g., 48 hours or 72 hours).	X	X	X	X					UPICs
10591.25	The UPICs and National Benefit Integrity Medicare Drug Integrity Contractor (MEDIC) shall follow the vulnerabilities process, as descibed in section 4.31, Chapter 4, Pub. 100-08.									MEDIC, UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
10591.26	The UPICs, RACs, MACs, and SMRC shall follow the RAC Data Warehouse coordination process, as described in section 4.33, Chapter 4, Pub. 100-08.	X	X	X	X					RAC, SMRC, UPICs
10591.26.1	The UPICs shall review the RAC Data Warehouse to determine if other contractors currently have a particular provider under review.									UPICs
10591.26.2	If the provider is under review by another contractor, the UPIC shall contact that respective contractor to determine which entity should continue to review that provider and how to handle the current medical review.									UPICs

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: N/A

"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): Jesse Havens, 410-786-6566 or jesse.havens@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. 851, Issued: 12-14-18)

Transmittals for Chapter 4

4.1 - Introduction

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The CMS Pub. 100-08, Program Integrity Manual (PIM), reflects the principles, values, and priorities of the Medicare Integrity Program (MIP). The primary principle of program integrity (PI) is to pay claims correctly. To meet this goal, *Unified* Program Integrity Contractors (*UPIC*s) and Medicare Administrative Contractors (MACs) must ensure that Medicare pays the right amount for covered and correctly coded services rendered to eligible beneficiaries by legitimate providers. *The focus of the UPICs and MACs shall be to ensure compliance with Medicare regulations, refer suspected fraud and abuse to our Law Enforcement (LE) partners, and/or revocation of providers that are non-compliant with Medicare regulation and policies.* The Centers for Medicare & Medicaid Services (CMS) follows four parallel strategies in meeting this goal:

1. Prevent 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 closely with partners, including other *UPIC*s, MACs, LE agencies, and State Program Integrity units; and

4. Enact fair and firm enforcement policies.

The *UPIC*s shall follow the PIM to the extent outlined in their respective task orders' Statement of Work (SOW). The *UPIC*s shall only perform the functions outlined in the PIM as they pertain to their own operation. The *UPIC*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 *that* all *UPICs* are awarded, any reference to *UPIC*s shall also apply to *Zone Program Integrity Contractors (ZPICs)*, unless otherwise noted *or identified* in the *Z*PIC SOW. MACs shall follow the PIM in accordance with their SOW.

4.2 - Medicare Program *Integrity*

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s and MACs, as indicated.

The primary goal of the *UPIC* 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 examples of the actions that may be taken *in cases of suspected fraud*. Once such actions are taken, cases where there is potential fraud are referred to *law enforcement* for consideration and initiation of criminal or civil prosecution, civil monetary penalties, or administrative sanction actions.

Preventing and detecting fraud, waste, and abuse involves a cooperative effort among beneficiaries; *UPIC*s; MACs; providers/suppliers; quality improvement organizations (QIOs); 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 *UPIC* 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 *UPIC* makes the determination of potential fraud, waste, *and/*or abuse, the *UPIC* shall effectuate all appropriate administrative actions and refer the case to *law enforcement*, if appropriate.

When the *UPIC* makes the determination that a *matter* is not potential fraud*, waste, and/or abuse*, the *UPIC* shall close the matter, or *de-escalate* the *matter* to the appropriate unit at the MAC, QIO, or other entity, when appropriate.

4.2.1 - Examples of Medicare Fraud

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s 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 for 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 a*nd a beneficiary;*

- 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);

- Misrepresenting 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;

- *Knowingly allows a beneficiary to use* 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 arrangements 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 certain hospital-based physician arrangements;

- Paying amounts 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;

- Depreciating assets that have been fully depreciated or sold;

- Using depreciation methods not approved by Medicare;

- Repaying interest expense for loans that were for an offset of interest income against the interest expense;

- Reporting program data where provider program amounts cannot be supported;

- Allocating costs improperly related to organizations that have been determined to be improper; or

- Manipulating accounting.

4.2.2 - *Unified* Program Integrity Contractor

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

The *UPIC* is responsible for preventing, detecting, and deterring fraud, waste, and abuse in both the Medicare program and the Medicaid program. The *UPIC*:

- 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. *When appropriate, the UPIC may collaborate with CMS, State Medicaid Agency, and MFCU personnel*;

- Explores all available sources of fraud leads in its *jurisdiction*, 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 in *suspected Medicaid fraud, waste, and abuse cases (including* Medi-Medi *cases)*; or

- Works closely with CMS on joint projects, investigations and other proactive, anti-fraud activities.

The *UPIC* 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 UPIC*. Examples of proactive leads include, but are not limited to: (1) *UPIC* 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 *UPIC* during a provider/supplier or beneficiary interview; and (3) the combining of information from a variety of sources to create a new lead. The *UPIC* shall pursue leads identified through data analysis (*UPIC*s shall follow PIM chapter 2, section 2.3 for sources of data), the Internet, the Fraud Investigation Database (FID), *the Unified Case Management system (UCM)*, news media, industry workgroups, conferences, etc. For workload reporting purposes, the *UPIC* shall only identify as proactive those investigations and cases that the *UPIC* self-initiated.

The *UPIC* 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 *UPIC* data is proactive.

4.2.2.1 - Organizational Requirements

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s and MACs, as indicated.

UPIC 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.

The UPIC shall follow the requirements in its UPIC SOW for prioritizing leads. UPIC PI managers shall prioritize work coming into the *UPIC* to ensure that investigations with the greatest program impact and/or urgency are given the highest priority. The *UPIC* shall prioritize all work on an ongoing basis as new work is received. The *UPIC* 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.

Allegations having the greatest program impact *and priority* would include investigations cases involving, *but not limited to*:

- Patient abuse or harm
- Multi-state fraud
- High dollar amounts of potential overpayment *or potential for other admin actions, e.g. payment suspensions and revocations*
- 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 *UPIC* 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 *UPIC* 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 *Unified* Program Integrity Contractor Employees

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

Under the terms of their contracts (refer to 42 CFR §421.316(a)), *UPIC*s, 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 *UPIC* 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 *UPIC* 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 *UPIC* is served with a complaint, the *UPIC* shall immediately contact its chief legal counsel and the COR. The *UPIC* shall forward the complaint to the HHS Office of the Regional Chief Counsel (the CMS regional attorney) who, in turn, will notify the U.S. Attorney's office. The HHS Office of the Regional Chief

Counsel and/or the COR will notify the *UPIC* 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. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

All levels of *UPIC* 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 *UPIC* 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. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

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

4.2.2.4 - Procedural Requirements

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s 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 *UPIC*. Any area within the MAC (e.g., MR, enrollment, screening staff) that refers potential fraud, waste, and abuse to the *UPIC* 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 *UPIC*, name and contact information of the individual who made the referral, and the name of the *UPIC* 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 include provisions to ensure that personnel shall:

- Refer potential fraud, waste, or abuse situations promptly to the *UPIC*;
- Forward complaints alleging fraud through the screening staff to the *UPIC*;
- Maintain confidentiality of referrals to the *UPIC*;
- Forward to the *UPIC* 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 *UPIC* 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 *UPIC*s 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 *UPIC* 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, *UPIC*s, 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 units 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 *UPIC*.

• 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 *UPIC* 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 *UPIC* personnel in the proposed onsite visit. The potential harm to the case and the safety of *UPIC* personnel shall be thoroughly evaluated. The *UPIC* personnel shall properly identify themselves as *UPIC* employees and under no circumstances shall they represent themselves as LE personnel or special agents. Lastly, under no circumstances shall *UPIC* 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. *The UPIC is expected to follow the current vetting process and the requirements of PIM Sections 4.41 G, K and L. The UPIC shall consult with the BFLs and CORs if questions arise about complying with LE requests for medical records, conducting interviews, or refraining from specific administrative actions.*

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., Senior Medicare Patrols), and other CMS health care partners (e.g., Administration on Aging (AoA), state MFCUs).

• 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 *UPIC* 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. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall maintain files on providers/suppliers who have been the subject of complaints, prepayment edits, *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* shall ensure that all evidentiary documents are kept free of annotations, underlining, bracketing, or other emphasizing pencil, pen, or similar marks.

The UPIC shall establish an internal monitoring and investigation review system to ensure the adequacy and timeliness of fraud, waste, and abuse activities. *The UPIC shall maintain their workload in the Unified Case Management (UCM) system, unless otherwise directed by CMS.*

4.2.2.4.2 - File/Document Retention

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

Files/documents shall be retained for 10 years. However, files/documents shall be retained indefinitely and shall not be destroyed if they relate to a current investigation or litigation/negotiation; ongoing Workers' Compensation set aside arrangements, or documents which prompt suspicions of fraud*, waste,* and*/or* abuse of overutilization of services. This will satisfy evidentiary needs and discovery obligations critical to the agency's litigation interests.

For UPIC's in transition, all existing electronic files for all years shall be transferred into UCM. Any hard copy files (that do not need to be retained indefinitely) older than 10 years shall be destroyed.

For UPICs in operation, all paper/hard copy files older than 10 years (that do not need to be retained indefinitely) shall be destroyed.

Any hard copy files older than 10 years that are part of a current investigation or litigation may be scanned as an electronic copy. After certification that it has been properly scanned, it shall be destroyed. All scanned/electronic copies shall be transferred to the UCM.

4.2.2.6 – Program Integrity Security Requirements

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

To ensure a high level of security for the *UPIC* functions, the *UPIC* 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 *UPIC* shall adequately inform and train all *UPIC* employees to follow *UPIC* security policies and procedures so that the information the *UPIC* obtain is confidential.

Note: The data *UPIC*s collect in administering *UPIC* contracts belong to CMS. Thus, the *UPIC*s collect and use individually identifiable information on behalf of the Medicare program to routinely perform the business functions necessary for administering 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 *UPIC*s shall follow. The requirements listed below are in the BPSSM or ARS. There are several exceptions. The first is requirement A (concerning *UPIC* 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. *Unified* Program Integrity Contractor Operations

- The *UPIC* shall conduct their activities in areas not accessible to the general public.

- The *UPIC* 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 *UPIC* 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 *UPIC* 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 includes (this is not an exhaustive list):

  – Appropriate CMS personnel

  – *UPIC* staff

  – MAC MR staff

  – *UPIC* or MAC audit staff

  – *UPIC* or MAC data analysis staff

  – *UPIC* or MAC senior management

  – *UPIC* 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 surroundings of a specific workstation or class of workstation that can access sensitive CMS information. CMS requires that for *UPIC*s all local workstations as well as workstations used at home by *UPIC*s comply with these requirements.

– If *UPIC* 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 *UPIC* shall also adhere to the following:

• Ensure the mailroom, general correspondence, and telephone inquiries procedures maintain confidentiality whenever the *UPIC* 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 *UPIC* mail in the mailroom unless the *UPIC* has requested the mailroom do so for safety and health precautions. Alternately, if mailroom staff opens *UPIC* mail, mailroom staff shall not read the contents.

• For mail processing sites separate from the *UPIC*, the *UPIC* shall minimize the handling of *UPIC* mail by multiple parties before delivery to the *UPIC*.

• The *UPIC* shall mark mail to CMS Central Office or to another *UPIC* "personal and confidential" and address it to a specific person.

• Where more specialized instructions do not prohibit *UPIC* 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 employees shall restrict access to sensitive and investigative materials, and *UPIC* staff shall not leave such material unattended.

• The *UPIC* staff shall safeguard all sensitive or investigative material when the materials are being transported or sent by *UPIC* staff.

• The *UPIC* 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, HICNs, 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 *UPIC* data) for additional requirements.

D. Staffing of the *Unified* Program Integrity Contractor and Security Training

The *UPIC* 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. (People with access to sensitive data at CMS have a level 5 risk). The *UPIC* may require investigations above a level 2 if the *UPIC* believes the higher level is required to protect sensitive information.

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

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

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

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

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

The *UPIC* shall notify the OIG if parties without a need to know are asking inappropriate questions regarding any investigations. The *UPIC*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 *UPIC*s shall implement phone security practices. The *UPIC*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 *UPIC* involved in the investigation of the related issue.

Additionally, the *UPIC*s shall only use CMS, the OIG, the DOJ, and the FBI phone numbers that they can verify. To assist with this requirement, *UPIC* management shall provide *UPIC* staff with a list of the names and telephone numbers of the individuals of the authorized agencies that the *UPIC*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, *UPIC*s shall not respond to questions concerning any case the OIG, the FBI, or any other LE agency is investigating. The *UPIC*s shall refer such questions to the OIG, the FBI, etc., as appropriate.

Finally, the *UPIC*s shall transmit sensitive and investigative information via facsimile (fax) lines only after the *UPIC* has verified that the receiving fax machine is secure. Unless the fax machine is secure, *UPIC*s shall make arrangements with the addressee to have someone waiting at the receiving machine while the fax is transmitting. The *UPIC*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.

4.2.3 - Durable Medical Equipment Medicare Administrative Contractor Fraud Functions

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC*s shall process all complaints alleging DMEPOS fraud *and abuse* that are filed in their regions/zones in accordance with requirements of PIM Chapter 4, §4.6.

The *PI* unit manager has responsibility for all *PI* unit activity, including the coordination with outside organizations as specified in the PIM, chapter 4, §4.4.

A. General Requirements

Since the Medicare program has become particularly vulnerable to fraudulent activity in the DMEPOS area, each *UPIC* shall:

- Routinely communicate with and exchange information with its MR unit and ensure that referrals for prepayment MR review or other actions are made.

- Consult with the *UPIC* medical directors in cases involving medical policy or coding issues.

- Fully utilize data available from the MAC with the pricing, data analysis and coding function (PDAC) to identify items susceptible to fraud.

- Keep the PDAC contractor, other *UPIC*s, *CORs, BFLs*, and SMEs informed of its ongoing activities and share information concerning aberrancies identified using data analysis, ongoing and emerging fraud schemes identified, and any other information that may be used to prevent similar activity from spreading to other jurisdictions.

4.3 – Medical Review for Program Integrity Purposes

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

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 *UPIC* 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 *UPIC*'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 *UPIC* 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 *UPIC*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 *UPIC* 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 *UPIC*'s analysis. Another option may be for the *UPIC* 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 *or Recovery Audit Contractor* to the *Unified* 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 *or RAC* personnel *may* discuss *potential referral of the* matter *to* the *UPIC*. If the *UPIC* agrees that there is potential fraud, *waste, and/or abuse,* the MAC *or RAC personnel shall escalate and refer the matter* to the *UPIC*.

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 *UPIC*.

The focus of MAC MR is to reduce the error rate through MR and provider/supplier notification and feedback. *The focus of the RAC is to identify and correct Medicare improper payments through detection and collection of overpayments. The focus of the UPIC is to* address situations of potential fraud, waste, and abuse.

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

The *UPIC*s are also responsible for preventing and minimizing the opportunity for fraud. The *UPIC*s 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 *UPIC*s and/or CMS to monitor specific beneficiary and/or provider/supplier numbers and other claims criteria. When appropriate, the *UPIC* may request the MAC to install a prepayment or auto-denial edit. The MACs shall comply with requests from *UPIC*s and/or CMS to implement those edits. The MACs shall implement parameters for those edits/audits within the timeframe established in the MAC and *UPIC* 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 *UPIC* staff is performing MR for PI purposes, its focus may be different (e.g., looking for possible falsification). The *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* shall have access to provider/supplier tracking systems from MR. The information on the tracking systems shall be used for comparison to *UPIC* findings. The *UPIC* shall also consider that the MR department may have established internal guidelines (see PIM, chapter 3).

3. The *UPIC* 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 *UPIC* 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 *UPIC* shall also verify diagnosis and match to age, gender, and procedure.

5. The *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* shall document errors found and communicate these to the provider/supplier in writing when the *UPIC*'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 *UPIC* 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 *UPIC* 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 *UPIC's* MR for PI program. In addition, the *UPIC* shall have in place procedures for continuous quality improvement in order to continually improve the effectiveness of their processes.

1. The *UPIC* 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 *UPIC* staff shall be able to request training on specific issues.

2. The *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* shall establish a Quality Improvement (QI) process that verifies the accuracy of MR decisions made by licensed health care professionals. *UPIC*s 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 *UPIC* evaluation results identify the need for prepayment edit placement at the MAC, the *UPIC* 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 *UPIC* to evaluate edits submitted at the request of the *UPIC*. The evaluation of edits shall consider the timing and staffing needs for reviews. The *UPIC* 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 *UPIC* 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. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

Federal, state, 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 *UPIC* disclose beneficiary records or provider/supplier information, the responsive disclosure shall comply with applicable federal law as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Business Associate provision of the *UPIC*'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, certain general information that does not include specific beneficiary identifiers may be shared with a broader community, including private insurers. The 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 *UPIC* may release information, in accordance with the requirements specified in Sections A – G below, to the following organizations:

- Other *UPIC*s
- 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 *UPIC* 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, necessitating the tracking of any disclosures of information by the *UPIC*. The *UPIC* shall direct questions concerning what information may be disclosed under the Privacy Act or Privacy Rule to the CMS Regional Office Freedom of Information Act (FOIA)/privacy coordinator. Ultimately, the authority to release information from a Privacy Act System of Records to a third-party rests with the system manager/business owner of the system of records.

The HIPAA Privacy Rule establishes national standards for the use and disclosure of individuals' health information (also called protected health information [PHI]) by organizations subject to the Privacy Rule (which are called "covered entities"). As "business associates" of CMS, *UPIC*s 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 federal, state, 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 federal 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 *UPIC*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 *UPIC* 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, *UPIC*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 *UPIC* shall contact its COR and IAG BFL for further guidance.

B. Requests from Other *Unified* Program Integrity Contractors

The *UPIC*s may furnish requested specific information concerning ongoing fraud investigations and individually identifiable PHI to any *UPIC* or MAC. *UPIC*s 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 *UPIC* shall notify the OIG/OI of the request for information received from another *UPIC* and notify the requesting *UPIC* 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 *UPIC* review determination, it shall coordinate with the MAC to obtain all records and supporting documentation that the *UPIC* provided to the MAC in support of the MAC's first level appeals activities (redeterminations). As necessary, the QIC may also contact the *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* may furnish requested specific information concerning ongoing fraud investigations containing personally identifiable information to the QIOs and state survey and certification agencies. The functions QIOs perform for CMS are required by law; thus the Privacy Rule permits disclosures to them. State survey and certification agencies are required by law to perform inspections, licensures, and other activities necessary for appropriate oversight of entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; thus the Privacy Rule permits disclosures to them. If the request concerns cases already referred to the OIG/OI, *UPIC*s shall refer the requestor to the OIG/OI.

E. Requests from State Attorneys General and State Agencies

The *UPIC* may furnish requested specific information on ongoing fraud investigations to state Attorneys General and to state agencies. Releases of information to these entities in connection with their responsibility to investigate, prosecute, enforce, or implement a state statute, rule, or regulation may be made as a routine use under the Privacy Act of 1974, as amended; 5 USC §552a(b)(3) and 45 CFR Part 5b Appendix B (5). 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 *UPIC* 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 *UPIC* shall refer the requestor to the OIG/OI.

F. Requests from Medicaid Fraud Control Units

Under current Privacy Act requirements applicable to program integrity investigations, the *UPIC* 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 state statute, rule or regulation may be made as a routine use under the Privacy Act of 1974, as amended; 5 USC §552a(b)(3) and 45 CFR Part 5b Appendix B (5). 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 *UPIC* may, at its discretion, share PIM Exhibit 25 with the requestors as a template to assist them in preparing their request. If the request concerns cases already referred to the OIG/OI, the *UPIC* shall refer the requestor to the OIG/OI.

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

The *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC*'s files unless an exception exists as described below.
The *UPIC* 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 *UPIC* within 20 calendar days of receipt of the request from the *UPIC* unless there are extenuating circumstances. The MAC shall communicate any extenuating circumstances to the *UPIC* and the MAC COR as soon as they become known. The *UPIC* shall communicate these extenuating circumstances to its COR.

Periodically, there are instances where the OIG/OI is in need of the requested information in a shorter timeframe than (30) calendar days. To account for these instances, the UPIC and MAC may add language to their Joint Operating Agreement that allows for a shorter timeframe for the MAC to furnish the requested information (i.e. 48 hours, 72, hours, etc.). In these instances, the OIG/OI must provide justification as to why the requested information is needed in a shorter timeframe than the standard Priority I request.

*Otherwise, t*he *UPIC* 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 *UPIC* from meeting the thirty (30) day timeframe, the *UPIC* shall inform the requestor what, if any, portion of the request can be provided within thirty (30) days. The *UPIC* shall notify the requesting office as soon as possible (but not later than thirty (30) days) after receiving the request. The *UPIC* 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 *UPIC* 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 *UPIC* shall inform the requestor what, if any, portion of the request can be provided. The *UPIC* shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested.

The *UPIC*s shall respond to such requests within 45 calendar days or sooner, when possible. The MAC shall furnish requested information to the *UPIC* within 30 calendar days of receipt of the request from the *UPIC* unless there are extenuating circumstances. The MAC shall communicate any extenuating circumstances to the *UPIC* and the MAC COR as soon as they become known. The *UPIC* shall communicate these extenuating circumstances to its COR. The *UPIC* 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 *UPIC* from meeting the 45-day timeframe, the *UPIC* shall inform the requestor what, if any, portion of the request can be provided within 45 calendar days. The *UPIC* shall notify the requesting office as soon as possible (but not later than 45 calendar days) after receiving the request. The *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* shall obtain approval from the COR regarding requests started by the *UPIC* that they subsequently anticipate will exceed that 40-hour level of effort. The *UPIC* 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 *UPIC*s 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 *UPIC* 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 designees such as analysts, auditors, investigators, or paralegals). 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 *UPIC*, 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 *UPIC* shall discuss the information needed by the DOJ and determine the most efficient and timely way to provide the information. When feasible, the *UPIC* 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 *UPIC* shall obtain and transmit relevant statistical information to the DOJ (as soon as possible but no later than five (5) calendar days). The *UPIC* 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 *UPIC* with existing DOJ guidance (Exhibit 15).

The *UPIC* shall provide data to the DOJ, when feasible, in a format to be agreed upon by the *UPIC* 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 emergency requests, which require coordination with Headquarters, the DOJ, and CMS staff. These 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 *UPIC*'s files unless an exception exists as described below.

The *UPIC* 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 *UPIC* within 20 calendar days of receipt of the request from the *UPIC* unless there are extenuating circumstances. The MAC shall communicate any extenuating circumstances to the *UPIC* and the MAC COR as soon as they become known. The *UPIC* shall communicate these extenuating circumstances to its COR.

Periodically, there are instances where the DOJ is in need of the requested information in a shorter timeframe than (30) calendar days. To account for these instances, the UPIC and MAC may add language to their Joint Operating Agreement that allows for a shorter timeframe for the MAC to furnish the requested information (i.e. 48 hours, 72, hours, etc.). In these instances, the DOJ must provide justification as to why the requested information is needed in a shorter timeframe than the standard Priority I request.

Otherwise, the UPIC 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 *UPIC* from meeting the thirty (30) day timeframe, the *UPIC* shall inform the requestor what, if any, portion of the request can be provided within thirty (30) days. The *UPIC* shall notify the requesting office as soon as possible (but not later than thirty (30) days) after receiving the request. The *UPIC* 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 *UPIC* 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 *UPIC* shall inform the requestor what, if any, portion of the request can be provided. The *UPIC* shall provide the relevant data, reports, and findings to the requesting agency in the format(s) requested.

The *UPIC* shall respond to such requests within 45 calendar days or sooner, when possible. The MAC shall furnish requested information to the *UPIC* within 30 calendar days of receipt of the request from the *UPIC* unless there are extenuating circumstances. The MAC shall communicate any extenuating circumstances to the *UPIC* and the MAC COR as soon as they become known. The *UPIC* shall communicate these extenuating circumstances to their COR. The *UPIC* 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 *UPIC* from meeting the 45-day timeframe, the *UPIC* shall inform the requestor what, if any, portion of the request can be provided within 45 calendar days. The *UPIC* shall notify the requesting office as soon as possible (but not later than 45 calendar days) after receiving the request. The *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* shall obtain approval from the COR regarding requests started by the *UPIC* that they subsequently anticipate will exceed that 40-hour level of effort. The *UPIC* shall not exceed the 40-hour level of effort until it receives COR approval.

I. Duplicate/Similar Requests for Information

If the *UPIC* receives duplicate or similar requests for information from OIG and DOJ, the *UPIC* shall notify the requestors. If the requestors are not willing to share the information, the *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* to review and interpret medical records for them, the *UPIC* 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 *UPIC* 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 *UPIC* has resources to fulfill the request. If so, the request may be approved.

If LE requests the *UPIC* to perform MR on all investigations the *UPIC* initiates, the *UPIC* shall perform MR if it deems it necessary, on a case-by-case basis. The *UPIC* 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 *UPIC* Audits of Medicare Provider Cost Reports Relating to Fraud

If LE requests the *UPIC* to perform an audit of a Medicare provider's cost report for fraud, the *UPIC* shall consult with the MAC to inquire if an audit of the cost report has already been performed. The *UPIC* shall also consult with the COR and IAG BFL. The *UPIC* 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 *UPIC* shall perform the audit within the time frame and cost agreed upon with LE.

M. Requests from Law Enforcement for Information Crossing Several *UPIC Jurisdictions*
If a *UPIC* receives a request from LE for information that crosses several *UPIC* zones, the *UPIC* shall contact its COR and IAG BFL. In the event that multiple zones are providing information in connection with the request, each *UPIC* 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 *UPIC* to process these requests.

4.4.2 - *Unified* Program Integrity Contractor Coordination with Other *Unified* Program Integrity Contractors

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

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

4.4.2.1 - *Unified* Program Integrity Contractor Coordination with Other Entities

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

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

If the *UPIC* 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.

4.6.1 - Definition of a Complaint

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s and MACs.

A complaint is a statement, oral or written, alleging that a provider, supplier, or beneficiary *billed for and/or* 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 beneficiary 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 *UPIC* shall refer complaints alleging poor quality of care to the Medicare/Medicaid survey and certification agencies and the QIOs within two (2) business days. The *UPIC* 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 *UPIC* is necessary.

4.6.2 - Complaint Screening

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPICs*, Beneficiary Contact Center, and MACs, as indicated.

4.6.2.1 *– Contact Center Operations*

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The Contact Center Operations (CCO) is a CMS managed contact center which provides beneficiaries with personalized Medicare information and accepts both inquiries and complaints regarding a variety of topics including, but not limited to, billing errors, the provision of services/tests, and coverage guidelines.

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

• Lab Tests - CSRs shall ask callers if they recognize the referring physician. If they do, remind callers that the referring physician may have ordered some lab work for them. The beneficiaries 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 beneficiaries 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 processes.

• Billing Errors - If the beneficiaries 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 beneficiaries 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 (PTAN) (e.g., blood pressure check, injections). These services may be billed under the minimal evaluation and management codes.

• Billing Address vs. Practice Location Address - The CSR shall check the practice location address 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 use claim history files to determine if the complaint or inquiry needs to be referred *to the MAC for additional* screening.

Any provider/supplier inquiries regarding potential fraud, waste, and abuse shall be *referred* immediately to the *MAC for handling and* screening.

Immediate advisements *(IA)* shall be *referred* immediately to the MAC for handling *and screening*. These advisements include inquiries or allegations by beneficiaries or providers/suppliers concerning kickbacks, bribes, or a crime by a federal 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.

4.6.2.2. – OIG Hotline

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

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 CMS by the OIG. CMS will conduct an initial screening of the complaints received to determine which MAC should receive the complaint referral (Initial screening of the complaint and assignment to the MAC will be based solely upon the information provided to CMS by the OIG). CMS will then email the complaint to the appropriate MAC via the OIG Hotline Referral mailbox established by the relevant MAC. The email will contain the OIG Hotline Complaint Referral Template and any supporting documentation, if available. The OIG Hotline Complaint Referral Template will be populated with information relevant to the complaint. Due to the varying information obtained from each complaint, some fields within the template may appear blank because the information for the specific data field was not reported to the OIG Hotline. Should the UPIC receive an OIG Hotline

complaint directly from the OIG, the UPIC shall proceed with the necessary screening, vetting, and investigative steps, as described in sections 4.6.3, 4.6.4, and 4.6.5 of this chapter.

4.6.2.3 – MAC Complaint Screening

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

A. MAC Screening of CCO Referrals

The MAC shall only screen potential fraud, waste, and abuse complaints, inquiries referred by the CCO with a paid amount of $100 or greater (including the deductible as payment), or three (3) or more beneficiary complaints or inquiries, regardless of dollar amount, about the same provider/supplier. Complaints or inquiries that do not meet the above threshold for screening shall be closed. Each complaint or inquiry 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. The MAC shall enter all potential fraud, waste, and abuse complaints or inquiries received from beneficiaries into their internal tracking system. The MAC shall maintain a log of all potential fraud, waste, and abuse complaints or inquiries received from the CCO. At a minimum, the log shall include the following information:

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

The MAC staff may 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. The MAC 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 records shall be forwarded to the UPIC for review in accordance with the referral timeframe identified below.

When a complaint meeting the criteria of an IA or potential fraud, waste or abuse is received, the MAC shall not perform any screening but shall prepare a referral package within ten (10) business days of when the inquiry or IA was received, except for instances of potential patient harm, of which a referral package shall

be prepared by the end of the next business day after the inquiry or IA was received, and send it to the UPIC during the same timeframe using the guidelines established in section 4.6.2.4 – Referrals to the UPIC. Once the complaint has been referred to the UPIC, the MAC shall close the complaint in its internal tracking system.

B. Screening of OIG Hotline Referrals

The MAC shall screen every OIG Hotline complaint received from CMS to determine if the complaint can be closed, resolved, other appropriate action taken by the MAC, or referred to either another contractor, a State Medicaid Agency, or Marketplace Integrity. If the MAC determines that a referral shall be made, the MAC shall adhere to the referral guidelines established below and in 4.6.2.4 – Referrals to the UPIC.

All OIG Hotline complaints sent to the MAC by CMS shall be reviewed, determinations shall be made, and final action shall be taken within 45 business days from the date the complaint is received, unless medical records have been requested and the MAC is pending receipt of the records. The MAC shall use the date contained in the e-mail from CMS as the start of the 45 business day timeframe.

If, the MAC requests medical records and those records are not received within 45 business days, the MAC shall deny the claim(s) or keep the request open beyond the 45 business day timeframe to allow for receipt of the requested records, whichever is appropriate.

If fraud is suspected when medical records are not received or the MAC determines otherwise that the complaint or inquiry indicates potential fraud, waste, and abuse, the MAC shall forward it to the UPIC for further development within 45 business days of the date of receipt from CMS or within 30 business days of the date of receipt of medical records and/or other documentation, whichever is later. If a referral shall be made, the MAC shall adhere to the referral guidelines established below and in 4.6.2.4 – Referrals to the UPIC.

If the MAC determines that the complaint or inquiry is not a fraud and/or abuse issue, and if the MAC 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.

When a complaint meeting the criteria of an IA or potential fraud, waste or abuse is received, the MAC shall not perform any screening but shall prepare a referral package within ten (10) business days of when the inquiry or IA was received, and send it to the UPIC during the same timeframe using the guidelines established in 4.6.2.4 – Referrals to the UPIC. Once the complaint has been referred to the UPIC, the MAC shall close the complaint in its internal tracking system.

If the MAC receives a complaint from CMS 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.

MACs may receive complaints alleging fraud, waste or abuse in the Medicaid program. Upon receipt, the MAC shall refer the complaints to the appropriate Program Integrity Unit (PIU) within the State Medicaid Agency (SMA) noted in Exhibit 47.

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 MAC 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 only be required to close a complaint from the OIG Hotline in its internal tracking system and will no longer refer complaints that do not allege fraud, waste, or abuse involving CMS programs to the OIG.

If the MAC receives duplicate complaints, the second duplicate complaint shall be closed and cross-referenced to the original complaint. Subsequent complaints will be thoroughly reviewed to ensure that any new information is added to the original complaint. This will ensure all items in question related to the complaint are addressed. When the complaint is closed, monetary actions (if involved) shall only be claimed on the primary complaint.

4.6.2.4 Referrals to the UPIC

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

MACs that refer a complaint to the UPIC shall notify the UPIC 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 UPIC and shall send the complaint via a secure method such as e-mail or mail directly to the UPIC.

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

- *Claims may have been altered*
- *Claims have been up-coded to obtain a higher reimbursement amount and appear to be fraudulent or abusive;*
- *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). An example of an attempt to obtain duplicate reimbursement 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. This apparent double-billing does not include routine assignment violations. The MAC shall attempt to resolve all routine assignment violations. However, referral from the MAC to the UPIC shall be made in instances where the provider/supplier has repeatedly committed assignment violations, 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 submissions 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 UPIC 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 UPIC for review, the MAC shall prepare a referral package that includes, at a minimum, the following:

- *Provider/supplier name, NPI, 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 UPIC 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).*

The MAC shall maintain a copy of all referral packages.

4.6.2.5 – Unified Program Integrity Contractor Responsibilities
(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

When the complaint is received from the MAC screening staff, the UPIC 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 screening staff, or within 30 business days of receiving medical records and/or other documentation, whichever is later, to the UPIC. The UPIC shall send the acknowledgement letter within 15 calendar days of receipt of the complaint referral from the MAC screening staff, unless it can be resolved sooner. The letter shall be sent on UPIC letterhead and shall contain the telephone number of the UPIC analyst handling the case.

If the UPIC 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 screening. The MAC screening staff shall track the complaints returned by the UPIC. However, the UPIC 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 UPIC shall track complaints referred by the MAC screening area in the UPIC's internal tracking system.

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

4.6.3 - Screening Leads

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

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

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

Activities that the *UPIC* 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 *UPIC* may contact the provider directly to resolve only the assignment violation issue. If there are circumstances noted in FID*/UCM* that would raise additional concerns, the *UPIC* shall contact its COR and IAG BFL for further guidance. If the lead involves potential patient harm, the *UPIC* shall immediately notify CMS within two (2) business days.

After completing its screening, the *UPIC* shall close the lead if it does not appear to be related to fraud, waste, or abuse. Prior to closing the lead, the *UPIC* 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 *UPIC* refers the information to the MAC is the last day of the screening.

At a minimum, the *UPIC* 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., reviewed records and substantiated amounts billed). Ensure 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 *UPIC*'s activities (i.e., referrals to other entities).

Additionally, if the screening process exceeds 21 calendar days, the *UPIC* 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. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

All leads and any new subjects that the *UPIC* determines warrant further investigation shall be vetted through CMS for approval before transitioning to an investigation. *The UPIC shall vet all applicable NPIs and Provider Identifiers associated with the provider or supplier's tax-identification number, when initially vetting the lead with CMS.* The *UPIC* shall submit the lead to CMS within two (2) business days of the *UPIC* determining that the lead should be transitioned into an investigation. For the submission to CMS, the *UPIC* shall use the designated CMS Vetting Form, which shall include, at a minimum, NPI, name, and practice location.

The *UPIC* shall only open investigations on leads that are approved by CMS. *Once the lead is approved by CMS, the UPIC shall notate the date the lead was initially vetted and approved by CMS in FID/UCM.* If the *UPIC* is instructed by CMS to close the lead without further action, the *UPIC* 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 *UPIC* investigation, it is determined that additional NPIs should be incorporated into the ongoing investigation, the *UPIC* 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.

If multiple contractors become involved with the investigation, the UPIC that initially vetted the lead with CMS shall become the lead contractor, unless otherwise specified by CMS. The lead contractor shall notify all applicable contractors of the date the lead was vetted and approved by CMS for investigation. Therefore, no additional vetting is required by the other participating contractors. The other participating contractors shall also notate the date the lead was initially vetted and approved by CMS in their applicable case tracking system(s).

4.7 - Investigations

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

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 *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC* 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 *UPIC*s 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 *UPIC*s shall refer potential fraud cases to LE, as appropriate, and provide support for these cases. In addition, the *UPIC*s 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 investigations that the providers/suppliers are subject to prior authorization by the MAC, the UPIC may request the MAC to release the prior authorization requirement prior to pursuing the investigation further.

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

4.7.1 – Conducting Investigations

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* 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 (*UPIC*s 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 *UPIC* 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 *UPIC* 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 *UPIC* decides 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 *UPIC* 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 *UPIC* determines that an overpayment exists solely on data analysis, the *UPIC* shall obtain COR and IAG BFL approval prior to initiating the overpayment.

Periodically, 100% overpayments are identified because the provider or supplier does not provide the UPIC with the required medical record documentation to conduct post-payment medical review. 100% overpayments are defined as all the claims in the UPIC's selected sample universe that are considered to be improperly billed and paid based on the lack of documentation received. These claims are therefore denied through post payment review.

In instances where the 100% denial is due to lack of documentation, the UPIC shall consult with its COR and BFL prior to initiation of overpayment notification actions, including any coordination with the MAC or notice to the provider/supplier. If approved, the UPIC shall coordinate the recovery actions with the MAC, who would be responsible for processing the overpayment demand to the provider or supplier. If denied, the UPIC shall follow the instructions provided by its COR and IAG BFL.

4.7.2 – Closing Investigations

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

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 *UPIC* and the matter is referred back to the MAC or to another CMS contractor for further review;
• If it is closed with administrative action(s);
• If the potential fraud is not substantiated; and/or
• If CMS declined a requested administrative action.

4.8 - Disposition of Cases Referred to Law Enforcement

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall refer investigations to law enforcement when it has substantiated allegations of fraud including, but not limited to, documented allegations that a provider, beneficiary, supplier, or other subject:

(a) engaged in a pattern of improper billing, (b) submitted improper claims with suspected knowledge of their falsity, or (c) submitted improper claims with reckless disregard or deliberate ignorance of their truth or falsity. Prior to making such referrals, the *UPIC* shall, unless otherwise instructed by CMS, effectuate all appropriate administrative actions, except for requesting the collection of an overpayment from the MAC that is directly related to the underlying reason for the referral. This definition of a case includes any and all allegations (regardless of dollar threshold or subject matter) where *UPIC* staff verifies that there is potential Medicare fraud (the allegation is likely to be true) and a referral to federal law enforcement (OIG, FBI, DOJ) has been performed. *UPIC*s do not prove fraud; such action is within the purview of the DOJ.

4.8.1 – Reversed Denials by Administrative Law Judges on Open Cases

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

If a case is still pending at the OIG, FBI, or AUSA, and denials are reversed by an Administrative Law Judge (ALJ), the *UPIC* should recommend to CMS that it consider protesting the ALJ's decision to the DHHS Appeals Council, which has the authority to remand or reverse the ALJ's decision. *UPIC*s should be aware, however, that ALJs are bound only by statutory and administrative law (federal regulations), CMS rulings, and National Coverage Determinations.

The *UPIC* shall consult with its COR and IAG BFL before initiating a protest of an ALJ's decision. They should be aware that the Appeals Council has only 60 days in which to decide whether to review an ALJ's decisions. Thus, CMS needs to protest the ALJ decision within 30 days of the decision, to allow the Appeals Council to review within the 60-day limit. The *UPIC* shall notify all involved parties immediately if it learns that claims/claim denials have been reversed by an ALJ in a case pending prosecution.

4.8.2 - Production of Medical Records and Documentation for an Appeals Case File

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

When the *UPIC* denies a claim and the provider, supplier, physician or beneficiary appeals the denial, the MAC shall request the medical records and documentation that the *UPIC* used in making its determination. The *UPIC* shall assemble the case file and send it to the MAC within five (5) calendar days. *If the MAC request is received outside of normal business hours or on an observed holiday that the UPIC is closed for business, the first calendar day will not be counted until the first business day after receipt of the request (i.e. if received on Saturday, the following Monday will be counted as the first calendar day).*

The *UPIC* shall include any position papers or rationale and support for its decision so that the appeals adjudicator can consider it during the appeals process. However, *UPIC*s shall be aware that an appeals case file is discoverable by the appellant. This means that the appellant can receive a complete copy of the case file. Since the provider may receive the case file, the *UPIC* shall consult with law enforcement before including any sensitive information relative to a case.
If the *UPIC* would like to be notified of an ALJ hearing on a particular case, the *UPIC* shall put a cover sheet in the case file before sending it to the MAC. The cover sheet shall state that the *UPIC* would like to be notified of an ALJ hearing and list a contact name with a phone and fax number where the contact can be reached. The cover sheet shall also include language stating, "PLEASE DO NOT REMOVE" to ensure it stays on the case file should the file be sent to the QIC. If the *UPIC* receives a notice of hearing, the *UPIC* shall contact the QIC immediately.

The QICs are tasked with participating in ALJ hearings; therefore, they are the primary Medicare contractor responsible for this function. *UPIC*s may participate in an ALJ hearing, but they shall work with the QIC to ensure that duplicative work is not being performed by both the *UPIC* and the QIC in preparation for the hearing. *UPIC*s shall never invoke party status. If the *UPIC* participates in a hearing, it shall be as a non-party. An ALJ cannot require participation in a hearing, whether it is party or non-party. If a UPIC receives a notice that appears contrary to this instruction, the *UPIC* shall contact the QIC and their primary COR and IAG BFL immediately.

4.9 - Incentive Reward Program

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

Section 203(b)(1) of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191) instructs the Secretary to establish a program to encourage individuals to report information on individuals and entities that are engaged in or have engaged in acts or omissions that constitute grounds for the imposition of a sanction under sections 1128, 1128A, or 1128B of the Social Security Act (the Act), or who have otherwise engaged in sanctionable fraud, *waste,* and*/or* abuse against the Medicare program under title XVIII of the Act.

The Incentive Reward Program (IRP) was established to pay an incentive reward to individuals who provide information on Medicare fraud, *waste,* and*/or* abuse or other sanctionable activities. The applicable regulations are in 42 CFR § 420.405.

4.9.1 - *UPIC* Responsibilities for the Incentive Reward Program

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s and MACs, as indicated.

For *UPIC*s and MACs, the IRP responsibilities explained below shall be worked out in the *UPIC* and MAC Joint Operating Agreement (JOA).

4.9.2 - Guidelines for Processing Incoming Complaints

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s and MACs, as indicated.

On or after July 8, 1998, any complaints received that pertain to a potentially sanctionable offense as defined by sections 1128, 1128A, or 1128B of the Act, or that pertain to those who have otherwise engaged in sanctionable fraud, *waste,* and*/or* abuse against the Medicare program under title XVIII of the Act, are eligible for consideration for reward under the IRP. The *UPIC* should consider the complainant for the reward program. Complaints may originate from a variety of sources such as the OIG Hotline, the *UPIC*, customer service representatives, etc. The *UPIC* and MAC shall inform their staff of this program to ensure that the staff will respond to or refer questions correctly. PIM, Exhibit 5 provides IRP background information to assist staff who handle inquiries.

The *UPIC* and MAC shall treat all complaints as legitimate until proven otherwise. The MAC shall refer potential fraud, waste, and abuse incoming complaints to the *UPIC* for investigation. Complaints shall either be resolved by the *UPIC* or, if determined to be a sanctionable offense, referred to the OIG for investigation. Complaints that belong in another *UPIC*'s zone shall be recorded and forwarded to the appropriate *UPIC*. All information shall be forwarded according to existing procedures.

If an individual registers a complaint about a Medicare managed care provider/supplier, *UPIC*s and MACs shall record and forward all information to:

Centers for Medicare & Medicaid Services
Centers for Medicare Management
Performance Review Division
Mail Stop C4-23-07
7500 Security Blvd.
Baltimore, MD 21244

4.9.3 - Guidelines for Incentive Reward Program Complaint Tracking

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

If the *UPIC* receives a related complaint and the complainant is eligible for an IRP, the *UPIC* shall notate the IRPs in the FID and coordinate with its COR and IAG BFL when issuance of the award is identified.

4.9.4 - Excluded Individuals

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The following individuals are not eligible to receive a reward under the IRP:

- An individual who was, or is, an immediate family member of an officer or employee of the Department of Health and Human Services, its *UPIC*s, MACs, or subcontractors, the Social Security Administration (SSA), the OIG, a state Medicaid agency, the DOJ, the FBI, or any other federal, state, or local law enforcement agency at the time he or she came into possession, or divulged information leading to a recovery of Medicare funds. Immediate family is as defined in 42 CFR 411.12(b), which includes any of the following:
  - Husband or wife
  - Natural or adoptive parent, child, or sibling
  - Stepparent, stepchild, stepbrother, or stepsister
  - Father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, or sister-in-law
  - Grandparent or grandchild.
- Any other federal or state employee, *UPIC*, MAC, or subcontractor, or DHHS grantee, if the information submitted came to his/her knowledge during the course of his/her official duties.
- An individual who received a reward under another government program for the same information furnished.
- An individual who illegally obtained the information he/she submitted.
- An individual who participated in the sanctionable offense with respect to which payment would be made.

4.9.6 - *Unified* Program Integrity Contractor Responsibilities

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

For *UPIC*s and MACs, the IRP responsibilities explained below shall be worked out in the Joint Operating Agreement.

4.9.6.1 - Guidelines for Processing Incoming Complaints

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

On or after July 8, 1998, any complaints received that pertain to a potentially sanctionable offense as defined by §§1128, 1128A, or 1128B of the Act, or that pertain to those who have otherwise engaged in sanctionable fraud*, waste,* and*/or* abuse against the Medicare program under title XVIII of the Act, are eligible for consideration for reward under the IRP. While the complainant may not specifically request to be included in the IRP, the *UPIC* should consider the complainant for the reward program. Complaints may originate from a variety of sources such as the OIG Hotline, the *UPIC*, customer service representatives, etc. *UPIC*s and MACs shall inform their staff of this program so they will respond to or refer questions correctly. PIM Exhibit 5 provides IRP background information to assist staff who handle inquiries. *UPIC*s and MACs shall treat all complaints as legitimate until proven otherwise. They shall refer incoming complaints to the *UPIC* for *further screening*. Complaints shall either be resolved by the *UPIC*, if determined to be a sanctionable offense, referred to the OIG for investigation.
Complaints that belong in another *UPIC*'s zone shall be recorded and forwarded to the appropriate *UPIC*. All information shall be forwarded to them according to existing procedures.

If an individual registers a complaint about a Medicare Managed Care provider, *UPIC*s and MACs shall record and forward all information to:

Centers for Medicare & Medicaid Services
Centers for Medicare Management

Performance Review Division
Mail Stop C4-23-07
7500 Security Blvd.
Baltimore, MD 21244

4.9.6.2 - Guidelines for Incentive Reward Program Complaint Tracking

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC*s shall continue to track all incoming complaints potentially eligible for reward in their existing internal tracking system. The following complainant information shall be included:

- Name;
- Health insurance claim number or Social Security number (for non-beneficiary complaints);
- Address;
- Telephone number; or

Any other requested identifying information needed to contact the individual.

The *UPIC* shall refer cases to the OIG for investigation if referral criteria are met according to PIM Chapter 4, §4.18.1 - Referral of Cases to the Office of the Inspector General (OIG). The case report shall also be forwarded to the OIG.

The *UPIC* shall enter all available information into the IRP tracking database. Information that shall be maintained on the IRP tracking database includes:

- Date the case is referred to the OIG.
- OIG determination of acceptance.
- If accepted by OIG, the date and final disposition of the case by the OIG (e.g., civil monetary penalty (CMP), exclusion, referral to DOJ).
- Any provider identifying information required in the FID, e.g., the Unique Physician Identification Number (UPIN).

The OIG has 90 calendar days from the referral date to make a determination for disposition of the case. If no action is taken by the OIG within the 90 calendar days, the *UPIC* should begin the process for recovering the overpayment and issuance of the reward, if appropriate.

4.9.6.3 - Overpayment Recovery

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall initiate overpayment recovery actions according to PIM Chapter 3, if it is determined an overpayment exist. Only MACs shall issue demand letters and recoup the overpayment.

4.9.6.4 - Eligibility Notification

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

After all fraudulently obtained Medicare funds have been recovered and all fines and penalties collected, if appropriate, the *UPIC* will send a reward eligibility notification letter and a reward claim form to the complainant by mail at the most recent address supplied by the individual. PIM Exhibit 5.1 provides a sample eligibility notification letter and Exhibit 5.2 provides a sample reward claim form that may be used as guides.

4.9.6.5 - Incentive Reward Payment

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

After the complainant has returned the reward claim form with appropriate attachments, the *UPIC* shall determine the amount of the reward and initiate payment. The reward payment should be disbursed to the complainant from the overpayment money recovered. Payments made under this system are considered income and subject to reporting under Internal Revenue Service tax law. No systems changes to implement these procedures are to be made.

For *UPIC*s, only the MAC shall make IRP payments. The *UPIC* shall provide the necessary documentation to the MAC to initiate the IRP payment.

4.9.6.6 - Reward Payment Audit Trail

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall maintain an audit trail of the disbursed check. The following data shall be included:

- Amount of the disbursed check
- Date issued
- Check number
- Overpayment amount identified
- Overpayment amount recovered
- Social Security number of complainant
- Party the complaint is against

The *UPIC* shall update the IRP tracking database to reflect disbursement of the reward check to the complainant, and the *UPIC* shall work with the MAC via the JOA to disburse the reward check.

4.9.7 - CMS Incentive Reward Winframe Database

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The IRP database was designed to track rewards that could be paid for information about fraud or abuse of the Medicare Trust Fund. Access to the IRP database is through the Winframe file server located at the CMS data center and is controlled through password and access codes. Cases can be entered into the IRP system by any *UPIC*, or managed care organization contractor, or by the OIG. When the *UPIC* refers a case to the OIG, for which the complaint is eligible for the IRP, they shall update the IRP system with all available information. The database contains the current status of all Medicare fraud/abuse cases pending reward. Some cases may be closed without a reward, based on final disposition of the case. *UPICs* and CMS ROs have oversight responsibility for this system. The database provides the following information:

- On-demand management reports
- Duplicate complaints submitted for reward
- Audit trail of overpayments recovered as a result of the reward program

The IRP database user instructions are found in PIM Exhibit 5.3.

4.9.8 - Updating the Incentive Reward Database

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPICs* shall be responsible for updating the incentive reward database on overpayment recovery and reward amounts. *UPICs* shall regularly follow up with the OIG to obtain information on recovery of complaints referred to them that originated from an IRP complainant. The *UPIC* shall follow up on referrals to the OIG when no action is taken within 90 calendar days. The tracking system database shall be updated as information becomes available. Updates shall be entered, at a minimum, on a quarterly basis.

The IRP screens may be viewed in PIM Exhibit 5.9.

4.10 - Fraud Alerts

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

Fraud Alerts are issued when circumstances arise that indicate a need to advise the *UPIC*s, MACs, law enforcement, state Medicaid agencies, and other appropriate stakeholders about an activity that resulted in the filing of inappropriate and potentially false Medicare claims. If the *UPIC* identifies the need for a Fraud Alert, it shall provide the COR and IAG BFL a summary of the circumstances. CMS will evaluate the need to issue a Fraud Alert. All Fraud Alerts will be disseminated by CMS to the appropriate stakeholders and supplied to the *UPIC*s in the FID. *Once the information is disseminated, the UPIC may send any questions related to the Fraud Alert to the COR and IAG BFL.*

4.11.2.3 – Initial Entry Requirements for DMEPOS Payment Suspensions

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

When one ZPIC implements a DMEPOS payment suspension, all of the ZPICs shall place that supplier under payment suspension as well*, unless otherwise directed by CMS*. However, instead of having each ZPIC enter separate payment suspensions in the FID to track the payment suspension, only one FID entry is made and all of the ZPICs shall update that entry with information from their zone. *The lead-UPIC identified during the initial vetting process will continue to be the lead-UPIC for the payment suspension, unless otherwise directed by CMS.* The Lead ZPIC shall enter all appropriate information into the FID Payment Suspension Module when requesting a payment suspension.

Fields required to be input in order to save a payment suspension in the FID are indicated in the payment suspension module. Required fields are also listed in the FID User Guide, which is located under the Help menu in the FID.

The ZPIC shall be responsible for ensuring that all data entered into the FID payment suspension module are entered correctly. This requirement includes the correct spelling of names and accuracy of addresses and identifiers entered.

4.13 - Administrative Relief from Program Integrity Review in the Presence of a Disaster

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

During a governmentally declared disaster, whether manmade or otherwise, the *UPIC* shall continue every effort to identify cases of potential fraud. Therefore, if the *UPIC* suspects fraud of a provider/supplier who cannot furnish medical records in a timely manner due to a disaster, the *UPIC* shall ensure that the provider/supplier is not attempting to harm the Medicare Trust Fund by taking an unreasonable amount of time to furnish records. The *UPIC* shall request and review verification documentation in all instances where fraud is suspected.

In the case of complete destruction of medical records/documentation where backup records exist, the *UPIC* shall accept reproduced medical records from microfiched, microfilmed, or optical disk systems that may be available in larger facilities, in lieu of the original document. In the case of complete destruction of medical records where no backup records exist, the *UPIC*s shall consult with its COR and IAG BFL to determine the appropriateness of the request to reconstruct the medical records. If the COR and IAG BFL determine that medical review is appropriate, the *UPIC* shall instruct providers/suppliers to reconstruct the records as completely as possible with whatever original records can be salvaged. Providers/suppliers should note on the face sheet of the completely or partially reconstructed medical record: “This record was reconstructed because of disaster.”

4.14 - Provider/Supplier Contacts by the *UPIC*

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

A *UPIC* may determine that the resolution of an investigation does not warrant administrative action and that an educational meeting with the provider/supplier is more appropriate. The *UPIC* shall inform the

provider/supplier of the questionable or improper practices, the correct procedure to be followed, and that continuation of the improper practice may result in administrative actions. The *UPIC* shall document contacts and/or warnings with written reports and correspondence to the provider/supplier and place them in the investigation file.

If the provider/supplier continues aberrant billing practices, the *UPIC* shall initiate the appropriate administrative actions. If the *UPIC* meets with a provider/supplier, the *UPIC* shall prepare a detailed report for the investigation file. The report shall include the information in A, B, and C below.

A. Background of Provider/Supplier (Specialty)

The *UPIC* shall include a list of all enterprises in which the subject had affiliations, the states where the provider/supplier is licensed, all past complaints, and all prior educational contacts/notices.

B. Total Medicare Earnings

The *UPIC* shall include a report of the subject provider's/supplier's total Medicare earnings for the past 12 months.

The report shall include the following:

- Earnings for the procedures or services in question;
- Frequency of billing for these procedures/services; and
- Total number of claims submitted for these procedures/services.

C. Extent of Review Performed

The *UPIC* shall include in the detailed report, to be placed in the investigative file, the number and type of reviews performed, as well as the specific information outlined below:

- A report of the review process, including methodologies utilized, reason for the review, and findings;
- Any administrative actions implemented (e.g., overpayments identified); and
- Recommendation(s).

D. Report of Meeting

The *UPIC* shall include information pertaining to the meeting(s) conducted with the provider/supplier. This report shall include the following:

- Minutes from the meeting describing the problems and/or aberrancies discussed with the provider/supplier and the education provided to the provider/supplier to correct those problems based on the UPIC's medical review.
- Copies of educational materials given to the provider/supplier before, during, or subsequent to the meeting.

E. Written Correspondence Regarding Non-compliance

Per the abuse of billing authority under 42 C.F.R. § 424.535(a)(8)(ii) for a pattern or practice of submitting claims that do not meet Medicare requirements and in an effort to fully inform providers of the potential administrative actions that may be imposed based on continued violations of Medicare policy, the below statement should be included in all post payment correspondence that include an error rate, and if applicable, other communications that identify non-compliant billings and inform the provider/supplier of their non-compliance with Medicare requirements:

In addition, we remind you that our regulation at 42 CFR § 424.535 authorizes us to revoke Medicare billing privileges under certain conditions. In particular, we note that per 42 CFR § 424.535(a)(8)(ii), CMS has the authority to revoke a currently enrolled provider's or supplier's Medicare billing privileges if CMS determines that the provider or supplier has a pattern or practice of submitting claims that fail to meet Medicare requirements.

4.15 - Reserved for Future Use

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

4.16 – MAC and *UPIC* Coordination on Voluntary Refunds

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s and MACs, as indicated.

Voluntary refund checks payable to the Medicare program shall not be returned to the provider/supplier, regardless of the amount of the refund. The *UPIC* shall communicate with the MAC staff responsible for processing voluntary refunds to obtain information on the checks received. The MAC shall refer to Pub. 100-06, Financial Management Manual, for instructions on processing and reporting unsolicited/voluntary refunds received from providers/physicians/suppliers.

The *UPIC* shall perform an investigation on any voluntary refund where there is suspicion of inappropriate payment or if a provider/supplier is under an active investigation.
Should the *UPIC* receive a voluntary refund check in error, the *UPIC* shall coordinate the transfer of voluntary refund checks to the MAC through the JOA.

Through the JOA, the *UPIC* shall establish a mechanism whereby the MAC notifies the *UPIC* on a regular basis of all voluntary refunds it received. The *UPIC* or MAC shall send one letter annually (calendar year) to any provider/supplier that submits a voluntary refund during that calendar year, advising the provider/supplier of the following:

"The acceptance of a voluntary refund in no way affects or limits the rights of the Federal Government or any of its agencies or agents to pursue any appropriate criminal, civil, or administrative remedies arising from or relating to these or any other claims."

The *UPIC* and MAC shall establish in the JOA which contractor sends the above language. The MACs may send the language above on a voluntary refund acknowledgement letter or on a Remittance Advice, if this capability exists.

The *UPIC* shall refer to section 4.4.1(G) and (H) of this chapter for law enforcement requests for voluntary refund information.

4.18.1 - Referral of Cases to the OIG/OI

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall identify cases of potential fraud and shall make referrals of such cases, as appropriate, to the OIG/OI, regardless of dollar thresholds or subject matter. Prior to making such referrals, the *UPIC* shall, unless otherwise instructed by CMS, implement any administrative actions, except for requesting the collection of an overpayment from the MAC that is directly related to the underlying reason for the referral. Matters shall be referred when the *UPIC* has documented allegations including, but not limited to, a provider, beneficiary, supplier, or other subject, a) engaged in a pattern of improper billing, b) submitted improper claims with suspected knowledge of their falsity, or c) submitted improper claims with reckless disregard or deliberate ignorance of their truth or falsity.

When a case has been referred to the OIG/OI, OIG/OI has 60 calendar days to accept or decline the referral. The *UPIC* shall continue to monitor the need for administrative action prior to the elapsing of the 60

calendar days. During this 60-day period, the *UPIC* shall refrain from implementing any additional administrative actions against the provider/supplier without CMS approval. The *UPIC* shall implement any additional administrative actions, if appropriate, to include issuing an overpayment demand to the MAC when:

• The OIG/OI does not accept the referral or the *UPIC* does not receive a response from the OIG/OI within 60 calendar days following a referral, and
Other law enforcement agencies do not accept the referral within 45 calendar days following such referral.

Once a referral has been made to the appropriate law enforcement agencies, law enforcement has either declined, returned or has not responded to the referral by the designated response timeframe, and the *UPIC* has effectuated and concluded all necessary administrative actions (to include demand of any overpayment), the *UPIC* shall close the case in the *UCM*.
When the OIG/OI conducts an investigation, it will usually initiate ongoing consultation and communication with the *UPIC* to establish evidence (i.e., data summaries, statements, bulletins) that a statutory violation has occurred. If the *UPIC* has completed all of the appropriate administrative actions to include referral of an overpayment to the MAC (if appropriate) and the case has been accepted by OIG, the *UPIC* shall still close the case and fulfill all other LE activities through the RFI process noted in section 4.4 of this chapter.

4.18.1.2 - Immediate Advisements to the OIG/OI

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall notify the OIG/OI of an immediate advisement within two (2) business days of identifying a lead or investigation that meets the following criteria. The *UPIC* shall maintain internal documentation on these advisements when it receives allegations with one or more of the following characteristics:

- Indications of *UPIC* or MAC employee fraud
- Allegations of kickbacks or bribes, discounts, rebates, and other reductions in price
- Allegations of a crime committed by a federal or state employee in the execution of their duties
- Indications of fraud by a third-party insurer that is primary to Medicare

For complaints received from the OIG Hotline, the *UPIC* shall not send an immediate advisement to the OIG/OI unless other information is available to the *UPIC* that is not contained in the initial OIG Hotline complaint.

The *UPIC* shall continue to develop the lead as appropriate. If the *UPIC* determines that a lead warrants further investigation, it shall follow the processes described above in section 4.6.4 of this chapter. If the *UPIC* already had an open investigation and refers the subject to OIG/OI as an immediate advisement, it shall follow the processes described above in section 4.7 of this chapter.

When an immediate advisement is required, all available documentation received with the allegation shall be forwarded to the OIG. The initial forwarding of the applicable information does not equate to the *UPIC* completing the full referral package as defined in the PIM (refer to PIM Exhibit 16.1) and does not equate to a referral to law enforcement.

4.18.1.3 - Payment Suspension

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall refer to PIM, chapter 8, for payment suspension instructions.

4.18.1.4 - OIG/OI *Referral and* Summary *Report*

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC shall* use the *Referral Fact Sheet Template* when preparing referral*s* to the OIG/OI. The *UPIC* shall forward the referral *directly* to the OIG, *shall send a copy of the referral to its BFL(s) and COR(s),* and shall retain a copy of the *referral* in the investigation *case* file.

The Referral Fact Sheet *Template* can be found in PIM Exhibit 16.1.

4.18.1.5 - Referral to Other Law Enforcement Agencies

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

If the OIG/OI declines a case that the *UPIC* believes has merit, the *UPIC* shall refer the case to other law enforcement agencies, such as the FBI or MFCU, as appropriate.

4.18.1.5.1 - Continue to Monitor Provider and Document Case File

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall not close a case simply because it is not accepted by OIG/OI. Since the subject is likely to continue to demonstrate a pattern of fraudulent activity, they shall continue to monitor the situation and to document the file, noting all instances of suspected fraudulent activity, complaints received, actions taken, etc. This will strengthen the case if it is necessary to take further administrative action or there is a wish to resubmit the case to OIG/OI at a later date. If the *UPICs* do resubmit the case to OIG/OI, they shall highlight the additional information collected and the increased amount of money involved.

4.18.1.5.2 - Take Administrative Action on Cases Referred to and Refused by OIG/OI

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPICs* take immediate action to implement appropriate administrative remedies, including the suspension or denial of payments, and the recovery of overpayments (see PIM, chapter 3). Because the case has been rejected by law enforcement, *UPIC*s shall consult with the *COR, BFL, or Suspension* SME concerning the imposition of suspension. They pursue administrative and/or civil sanctions by OIG where law enforcement has declined a case.

A. Denial/Referral Action for Erroneous Payment(s), Cases Not Meeting the Referral Threshold

Many instances of erroneous payments cannot be attributed to fraudulent intent. There will also be cases where there is apparent fraud, but the case has been refused by law enforcement. Where there is a single claim, deny the claim and collect the overpayment. Where there are multiple instances, deny the claims, collect the overpayment, and warn the provider. *UPICs* shall refer the provider, as appropriate, to provider relations, medical review, audit, etc.

4.18.1.5.3 - Refer to Other Law Enforcement Agencies

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

If the OIG/OI declines a case that the *UPIC* believes has merit, the *UPIC* may refer the case to other law enforcement agencies, such as the FBI, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), RRB/OIG, and/or the MFCU.

The *UPIC* should recommend administrative and/or civil sanctions (including exclusions) to the OIG where law enforcement has declined the case.

4.18.2 - Referral to State Agencies or Other Organizations

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall refer instances of apparent unethical or improper practices or unprofessional conduct to state licensing authorities, medical boards, the QIO, or professional societies for review and possible disciplinary action.

In each state there is a Medicare survey and certification agency. This agency is typically within the state's Department of Health. The survey agency has a contract with CMS to survey and certify institutional providers, indicating whether they meet or do not meet applicable Medicare health and safety requirements, called "conditions of participation." Providers not meeting these requirements are subject to a variety of adverse actions, including bans on new admissions to termination of their provider agreements. These administrative sanctions are imposed by the Regional Office, typically after an onsite survey by the survey agency.

The *UPIC*'s and the MAC's MR staffs shall confer before such referrals, to avoid duplicate referrals. The *UPIC* shall gather available information and leave any further investigation, review, and disciplinary action to the appropriate professional society or State board. Consultation and agreement between the *UPIC*'s and the MAC's MR staffs shall precede any referral to these agencies.

The *UPIC* shall notify its CORs and IAG BFL of these referrals.

4.18.3 - *UPIC*s and QIOs

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

Communication with the QIO is essential to discuss the potential impact of efforts to prevent abuse, as well as ensure efforts are made to improve quality of care and access to such care.
If potential patient harm is discovered during the course of screening a lead or through the investigation process, the *UPIC* shall refer those instances to the QIO, state medical board, or state licensing agency. In addition to making the appropriate referrals, the *UPIC* shall notify the COR and IAG BFL within two (2) business days once the potential patient harm issue is discovered.

If the *UPIC* refers a provider to the State licensing agency or medical society (i.e., those referrals that need immediate response from the State licensing agency), the *UPIC* shall also send a copy of the referral to the QIO.

If a claim has been reviewed by the QIO, the decision made is final and binding on CMS, and the specific decision rendered by the QIO shall not be overturned by the *UPIC*.

4.18.4 – Referral of Cases to the MAC

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

There are certain instances when the UPIC may refer cases to the MAC for review and additional education. At any time during the course of a review of a provider, the UPIC may determine that referral to the MAC is appropriate. Under certain circumstances, CMS may direct the UPIC to initiate a referral to the MAC at any time if deemed appropriate.

A. Situations When a Referral to the MAC is Appropriate

The following are examples of when it may be appropriate for the UPIC to submit a referral to the MAC:

- *During lead screening, the UPIC determines that there is not a potential fraud, waste, or abuse issue (e.g. MR, enrollment, claims processing).*
- *During lead screening, the UPIC determines that the risk for fraud, waste, or abuse is extremely low. Such a determination could be made based upon a low total amount of dollars at risk, information that the erroneous billing was unintentional or without a significant pattern.*
- *During the investigation, the only available outcome deemed appropriate by the UPIC at the time is the identification of an overpayment and no referral to law enforcement or other administrative actions are contemplated (i.e. revocation, payment suspension, etc.). The UPIC shall complete their*

review, calculate the overpayment, and refer the matter to the MAC for issuance of the overpayment and for potential education and/or MAC medical review.

If the UPIC refers a provider/supplier to the MAC, but subsequently receives additional information of potential fraud, waste, and/or abuse that warrants further UPIC review, the UPIC shall inform the MAC that they are re-opening the investigation of the provider/supplier.

B. Situations When a Referral to the MAC is Not Appropriate

There are certain instances when the UPIC may determine that it is not appropriate to refer cases to the MAC for review. During the investigation, the UPIC may determine that the provider has been previously educated on the same issue(s) and there is a potential for the UPIC to pursue other administrative actions and/or referral to law enforcement. In those instances, the UPIC shall continue to monitor for fraud, waste, and/or abuse.

4.19.1 - The *Unified* Program Integrity Contractor's and Medicare Administrative Contractor's Role

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The MAC shall be responsible for:

• Ensuring that no payments are made to provider/suppliers for a salaried individual who is excluded from the program. OIG, as it becomes aware of such employment situations, notifies providers that payment for services furnished to Medicare patients by the individual is prohibited and that any costs (salary, fringe benefits, etc.) submitted to Medicare for services furnished by the individual will not be paid. A copy of this notice is sent to the *UPIC* and to the appropriate RO.

The *UPIC* and the MAC shall work out the following in their JOA:

• Furnishing any available information to the OIG/OI with respect to providers/suppliers requesting reinstatement.
• Reporting all instances where an excluded provider/supplier submits claims for which payment may not be made after the effective date of the exclusion.

The *UPIC* shall also be responsible for:

• Contacting OIG/OI when it determines that an administrative sanction against an abusive provider/supplier is appropriate.
• Providing OIG/OI with appropriate documentation in proposed administrative sanction cases.

4.19.2 - Authority to Exclude Practitioners, Providers, and Suppliers of Services

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

Section 1128 of the Act provides the Secretary of DHHS the authority to exclude various health care providers, individuals, and businesses from receiving payment for services that would otherwise be payable under Medicare, Medicaid, and all federal health care programs. This authority has been delegated to the OIG.

When an exclusion is imposed, no payment is made to anyone for any items or services in any capacity (other than an emergency item or service provided by an individual who does not routinely provide emergency health care items or services) furnished, ordered, or prescribed by an excluded party under the Medicare, Medicaid, and all federal health care programs. In addition, no payment is made to any business or facility, e.g., a hospital, that submits claims for payment of items or services provided, ordered, prescribed, or referred by an excluded party.

The OIG also has the authority under §1128(b)(6) of the Act to exclude from coverage items and services furnished by practitioners, providers, or other suppliers of health care services who have engaged in certain forms of program abuse and quality of care issues. In order to prove such cases, the *UPIC* shall document a long-standing pattern of care where educational contacts have failed to change the abusive pattern. Isolated instances and statistical samples are not actionable. Medical *physician*s must be willing to testify.

Authority under §1156 of the Act is delegated to OIG to exclude practitioners and other persons who have been determined by a QIO to have violated their obligations under §1156 of the Act. To exclude, the violation of obligation under §1156 of the Act must be a substantial violation in a substantial number of cases or a gross and flagrant violation in one or more instances. Payment is not made for items and services furnished by an excluded practitioner or other person. Section 1156 of the Act also contains the authority to impose a monetary penalty in lieu of exclusion. Section 1156 exclusion actions and monetary penalties are submitted by QIOs to the OIG/OI.

Payment is not made for items and services furnished by an excluded practitioner or other person.

4.19.2.2 - Identification of Potential Exclusion Cases

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall review and evaluate abuse cases to determine if they warrant exclusion action. Examples of abuse cases suitable for exclusion include, but are not limited to:

- Providers who have a pattern of adverse QIO or MAC findings.

- Providers whose claims must be reviewed continually and are subsequently denied because of repeated instances of overutilization.

- Providers who have been the subject of previous cases that were not accepted for prosecution because of the low dollar value

- Providers who furnish or cause to be furnished items or services that are substantially in excess of the beneficiary's needs or are of a quality that does not meet professionally recognized standards of health care (whether or not eligible for benefits under Medicare, Medicaid, title V or title XX).

- Providers who are the subject of prepayment review for an extended period of time (longer than 6 months) who have not corrected their pattern of practice after receiving educational/warning letters.

- Providers who have been convicted of a program related offense (§1128(a) of the Social Security Act).

- Providers who have been convicted of a non-program related offense (e.g., a conviction related to neglect or abuse of a beneficiary, or related to a controlled substance) (§1128(a) of the Social Security Act).

Also, §1833(a)(1)(D) of the Act provides that payment for clinical diagnostic laboratory tests is made on the basis of the lower of the fee schedule or the amount of charges billed for such tests. Laboratories are subject to exclusion from the Medicare program under §1128(b)(6)(A) of the Act where the charges made to Medicare are substantially in excess of their customary charges to other clients. This is true regardless of the fact that the fee schedule exceeds such customary charges.

Generally, to be considered for exclusion due to abuse, the practices have to consist of a clear pattern that the provider/supplier refuses or fails to remedy in spite of efforts on the part of the *UPIC*, MAC, or QIO groups. An exclusion recommendation is implemented only where efforts to get the provider/supplier to change the pattern of practice are unsuccessful. The educational or persuasive efforts are not necessary or desirable when the issues involve life-threatening or harmful care or practice.

If a case involves the furnishing of items or services in excess of the needs of the individual or of a quality that does not meet professionally recognized standards of health care, *UPIC* shall make every effort to obtain reports confirming the medical determination of their medical review from one or more of the following:

- The QIO for the area served by the provider/supplier
- State or local licensing or certification authorities
- QIO committees
- State or local professional societies
- Other sources deemed appropriate

4.19.2.3 - Development of Potential Exclusion Cases

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

A. Case Considerations

When *UPICs* recommend cases to OIG/OI for exclusion, they shall consider:

- The nature and seriousness of the acts in question
- Actions taken to persuade the provider/supplier to abstain from further questionable acts
- The experience gained from monitoring payments to the provider/supplier after corrective action was taken
- The degree of deterrence that might be brought about by exclusion
- The effects of exclusion on the delivery of health care services to the community
- Any other factors deemed appropriate

In cases recommended to OIG/OI for exclusion where there has **not** been a conviction, see 42 U.S.C. 1320 a-7(b).

Documentation for excessive services and charges shall include the length of time that the problem existed and the dollars lost by the program. Documentation of excessive services or poor quality of care requires a medical opinion from a qualified physician who must be willing to testify. All cases involving excessive services or poor quality of care shall also contain documentation of prior unsuccessful efforts to correct the problem through the use of less serious administrative remedies.

B. Notification to Provider

If, as a result of development of potential fraud or abuse, a situation is identified that meets one or more of the criteria in PIM Chapter 4, §4.19.2.1, *UPIC* shall consult the OIG/OI/OCIG (Office of Counsel to the Inspector General) contact person. The OIG prepares and sends a written notice to the provider containing the following information:

- Identification of the provider.
- The nature of the problem.
- The health care services involved.

• The basis or evidence for the determination that a violation has occurred. In cases concerning medical services, make every effort to include reports and opinions from a QIO or a QIO committee, or a state/local professional society.

• The sanction to be recommended.

• An invitation to discuss the problem with *UPIC* and OIG/OI staff, or to submit written information regarding the problem.

• A statement that a recommendation for consideration of sanctions will be made to the OIG/OI within 30 days, if the problems are not satisfactorily resolved.

If the provider/supplier accepts the invitation to discuss the issues, *UPIC* shall make a report of the meeting for the record. This does not have to be a professionally transcribed report. Copies of the letter to the provider/supplier and the provider response, or the summary of the meeting, shall be in the file.

The *UPIC* shall refer cases that demonstrate a strong fraud potential to OIG/OI for investigation.

The *UPICs* notify OIG/OI of any cases that reach the level where a provider/supplier is notified of a problem in accordance with this section, even if the provider is convinced that there was a legitimate reason for the problem or that the problem has been corrected. *UPICs* do not refer these cases to OIG/OI unless requested to do so.

The *UPICs* document and refer cases involving harmful care as rapidly as possible. They handle OIG/OI requests for additional information as priority items.

C. Additional Information

Additional information that may be of value in supporting a proposal to exclude includes any adverse impact on beneficiaries, the amount of damages incurred by the programs, and potential program savings.

D. Mitigating Circumstances

Any significant factors that do not support a recommendation for exclusion or that tend to reduce the seriousness of the problem may be found in 42 CFR Part 1001 and are also considered. One of the primary factors is the impact of the sanction action on the availability of health care services in the community. *UPICs* shall bring mitigating circumstances to the attention of OIG/OI when forwarding their sanction recommendation.

4.19.2.4 - Contents of Sanction Recommendation

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall include in the sanction recommendation (to the extent appropriate) the following information:

• Identification of the subject, including the subject's name, address, date of birth, social security number, and a brief description of the subject's special field of medicine. If the subject is an institution or corporation, include a brief description of the type of services it provides and the names of its officers and directors.

• A brief description of how the violation was discovered.

• A description of the subject's fraudulent or abusive practices and the type of health service(s) involved.

• A case-by-case written evaluation of the care provided, prepared by the *UPIC*'s, or MAC's MR staff, which includes the patient's medical records. This evaluation shall cite what care was provided and why such care was unnecessary and/or of poor quality. (The reviewer may want to consult with someone from their RO *CCSQ*.) Medicare reimbursement rules shall not be the basis for a determination that the care was not medically necessary. The reviewer shall identify the specific date, place, circumstance, and any other relevant information. If possible, the reviewer should review the medical records of the care provided to the patient before and after the care being questioned.

NOTE: A minimum of 10 examples shall be submitted in support of a sanction recommendation under §1128(b)(6)(B). In addition, none of the services being used to support the sanction recommendations shall be over 2 years old.

• Documentation supporting the case referral, e.g., records reviewed, copies of any letters or reports of contact showing efforts to educate the provider, profiles of the provider who is being recommended for sanction, and relevant information provided by other program administrative entities.

• Copies of written correspondence and written summaries of the meetings held with the provider regarding the violation.

• Copies of all notices to the party.

• Information on the amount billed and paid to the provider for the 2 years prior to the referral.

• Data on program monies on an assigned/non-assigned basis for the last 2 years, if available.

• Any additional information that may be of value in supporting the proposal to exclude or that would support the action in the event of a hearing.

NOTE: All documents and medical records should be legible.

4.19.2.6.1 - Denial of Payment to Employer of Excluded Physician

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

If an excluded physician is employed in a hospital setting and submits claims for which payment is prohibited, the MAC surveillance process usually detects and investigates the situation.

However, in some instances an excluded physician may have a salary arrangement with a hospital or clinic, or work in group practice, and may not directly submit claims for payment. If this situation is detected, MACs:

• Contact the hospital/clinic/group practice and inform them that they are reducing the amount of their payment by the amount of federal money involved in paying the excluded physician

• Develop and refer to the *UPIC* as a CMP case.

Upon referral from the MAC, the *UPIC* shall finalize the case and refer it to the OIG.

4.19.4 - Reinstatements

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

A provider may apply for reinstatement when the basis for exclusion has been removed, at the expiration of the sanction period, or any time thereafter. *UPICs* shall refer all requests they receive for reinstatement to the Office of Investigation of the OIG. Also, they furnish, as requested, information regarding the subject

requesting reinstatement. OIG notifies the *UPIC* in the State where the subject lives/practices of all reinstatements.

4.19.4.1 - Monthly Notification of Sanction Actions

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The Medicare Exclusion Database is a standard format, cumulative exclusion database that contains information on all exclusions and reinstatement actions in Medicare, Medicaid, and other Federal health care programs. CMS receives this information from the Office of Inspector General monthly.

The *UPIC*s and MACs shall use the information contained in the MED and the GAO Debarment list to:

- Determine whether a physician/practitioner/provider or other health care supplier who seeks approval as a provider of services in the Medicare/Medicaid programs is eligible to receive payment

- Ensure that sanctioned providers are not being inappropriately paid

The dates reflected on the MED are the effective dates of the exclusion. Exclusion actions are effective 20 days from the date of the notice. Reinstatements or withdrawals are effective as of the date indicated.

The MED shows the names of a number of individuals and entities where the sanction period has expired. These names appear on the MED because the individual or entity has not been granted reinstatement. Therefore, the sanction remains in effect until such time as reinstatement is granted.

The *UPIC*s and MACs shall check their systems to determine whether any physician, practitioner, provider, or other health care worker or supplier is being paid for items or services provided subsequent to the date they were excluded from participation in the Medicare program. In the event a situation is identified where inappropriate payment is being made, they shall notify OIG and take appropriate action to correct the situation. Also, UPIC*s* shall consider the instructions contained in the CMP section of the PIM (PIM, chapter 4, §4.20).

The *UPIC*s shall work with MACs to document a process in the JOA to make the MAC aware of any payments to an excluded provider.

The MACs shall ensure that no payments are made after the effective date of a sanction, except as provided for in regulations at 42 CFR 1001.1901(c) and 489.55.

The MACs shall check payment systems periodically to determine whether any individual or entity who has been excluded since January 1982 is submitting claims for which payment is prohibited. If any such claims are submitted by any individual in any capacity or any entity who has been sanctioned under §§1128, 1862(d), 1156, 1160(b) or 1866(b) of the Act, *UPICs* shall forward them to OIG/OI.

Also, MACs shall refer to the RO all cases that involve habitual assignment violators. In cases where there is an occasional violation of assignment by a provider, they shall notify the provider in writing that continued violation could result in a penalty under the *Civil Monetary Penalty Law (*CMPL*)*.

4.20.1.2 - Purpose

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The central purpose of the CMP process is to promote compliance with the program rules and regulations. To achieve this, CMS and its *UPIC*s and MACs shall enforce the regulatory standards and requirements.

The MACs shall educate the industry and the public regarding compliance. *UPIC*s and MACs shall have a statutory obligation to ensure compliance with regulations. Therefore, the efforts of MACs to achieve compliance shall be directed toward promoting a clear awareness and understanding of the program through

education. When these efforts for achieving voluntary compliance have failed, formal enforcement action shall be referred to the appropriate agency.

4.20.1.4 - Administrative Actions

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC*s and MACs shall ensure that the program rules and regulations are being appropriately followed. If violations are noted (either through internal reviews or through a complaint process), MACs shall take the appropriate steps to inform and educate the provider of the non-compliance and encourage future compliance.

If, after a period of time, there is no significant change by the provider (the non-compliance continues), then a final warning notice of plans to propose a corrective action (such as a CMP) shall be issued by the MAC. This notice shall be sent by certified mail (return receipt required) to ensure its receipt by the provider. The notice shall indicate that previous notifications sent to the provider failed to correct the problem, and that this is a final warning. Additionally, it shall indicate that any further continuation of the non-compliance will result in the matter being forwarded to CMS or the OIG for administrative enforcement. While not specifically assessing a monetary penalty amount, the notice shall indicate that this is one type of sanction that may be applied.

4.20.3.1 - Referral Process to CMS

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

Compliance is promoted through both administrative and formal legal actions. Administrative compliance action shall first be attempted by MACs through education and warning letters that request the provider to comply with Medicare's rules and regulations. If the provider fails to take corrective action and continues to remain non-compliant, the MAC shall make a referral to the *UPIC* who shall forward it to the *COR and BFL*.

It is important for MACs to promote program compliance in their respective jurisdictions. The MACs shall ensure that all materials presented to providers through education, published bulletins, or written communication are clear and concise and accurately represent the facts of compliance versus non-compliance. Providers shall also be allowed the opportunity to present additional facts that may represent mitigating circumstances. *UPICs* shall consider this information in an objective manner before proceeding with a CMP referral to CMS.

When a *UPIC* elects to make a CMP referral to CMS, the initial referral package shall consist of a brief overview of the case; supportive documentation is not required at such time. The initial referral package shall consist of:

1. Identification of the provider, including the provider's name, address, date of birth, Social Security number, Medicare identification number(s), and medical specialty. If the provider is an entity, include the names of its applicable owners, officers, and directors.

2. Identification of the CMP authorities to be considered (use the authorities identified in PIM Chapter 4, §4.20.2.1).

3. Identification of any applicable Medicare manual provisions.

4. A brief description of how the violations identified above were discovered, and the volume of violations identified.

5. Total overpayments due the program or the beneficiary(ies), respectively.

6. A brief chronological listing of events depicting communication (oral and written) between the MAC and the provider.

7. A brief chronological listing of bulletins addressing the non-compliant area (starting with the bulletin released immediately prior to the first incident of non-compliance by the provider).

8. Any additional information that may be of value to support the referral.

9. The name and phone number of contacts at the *UPIC*.

Upon receipt of the above information, CMS staff will review the materials and *may* conduct follow-up discussions with the *UPIC* regarding the referral. *Typically, w*ithin 90 days of receipt of the referral, CMS will notify the *UPIC* of its decision to accept or decline the referral.

If CMS declines the referral, the *UPIC* shall communicate this to the MAC to continue in their efforts to educate and promote compliance by the provider. The *UPIC* shall also consider other (less severe) administrative remedies, which, at a minimum, may include revocation of assignment privileges, establishing prepayment or postpayment medical reviews, and referral of situations to state licensing boards or medical/professional societies, where applicable. In all situations where inappropriate Medicare payments have been identified, MACs shall initiate the appropriate steps for recovery.
If CMS accepts the referral, the *UPIC* shall provide any supportive documentation that may be requested, and be able to clarify any issues regarding the data in the case file or *UPIC* and MAC processes.

4.20.3.2 - Referrals to OIG

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

Upon discovery of any case that may implicate any of the OIG's delegated CMP authority, regardless of whether there is any other pending activity, or whether the fraud case was closed, *UPIC* shall contact the OIG/OI Field Office to discuss the potential case. If this contact results in a referral, the *UPIC* shall follow the same referral format as described in PIM, chapter 4, §4.18.1.4. If a referral is not made or a referral is declined, the *UPIC* shall consider other administrative remedies, which, at a minimum, may include revocation of assignment privileges, establishing prepayment or post payment medical reviews, and referral of situations to state licensing boards or medical/professional societies, where applicable. In all situations where appropriate Medicare payments have been identified, MACs shall initiate the appropriate steps for recovery.

The *UPIC* shall send to the OIG all cases, as appropriate, where an excluded provider or individual has billed or caused to be billed to the Medicare or Medicaid program for the furnishing of items or services after exclusion. Such misconduct is sanctionable under §1128A(a)(C)(1) of the Social Security Act.

The *UPIC* shall send to the CMS Provider Enrollment and Oversight Group all cases where *UPIC* believes that misuse has occurred of the Medicare name, symbols, emblems, or other violations as described in §1140 of the Social Security Act and in 42 CFR 1003.102(b)(7).

4.20.4 - CMS Generic Civil Monetary Penalties Case Contents

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The following information, if available, shall be included as part of the CMP case package and made available upon request by CMS:

1. Background information:

    a. All known identification numbers (*NPI, PTAN*, etc.).

b. Provider's first and last name or entity name (if subject is an entity, also include the full name of the principal operator).

c. Provider/*supplier*'s address (street, city, state, and zip code). If violator is an entity, identify address where principal operator personally receives his/her mail.

2. Copies of any interviews, reports, or statements obtained regarding the violation.

3. Copies of documentation supporting a confirmation of the violation.

4. Copies of all applicable correspondence between beneficiary and provider.

5. Copies of all applicable correspondence (including telephone contacts) between the MAC and provider.

6. Copies of provider's applicable bills to beneficiaries and/or MACs, and associated payment histories.

7. Copies of any complaints regarding provider and disposition of the complaint.

8. Copies of all publications (e.g., bulletins, newsletters) sent to provider by the *UPIC*, or MAC who discuss the type of violation being addressed in the CMP case.

9. Copies of any monitoring reports regarding the provider.

10. Name and telephone number of *UPIC* contact.

4.20.5.1 - Beneficiary Right to Itemized Statement

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The following is background information for developing specific CMS CMP cases:

Effective for services or items provided on or after January 1, 1999, §4311 of the Balanced Budget Act (BBA) provides that Medicare beneficiaries have the right to request and receive an itemized statement from their health care provider of service (e.g., hospital, nursing facility, home health agency, physician, non-physician practitioner, DMEPOS supplier). Upon receipt of this request, providers have 30 days to furnish the itemized statement to the beneficiary. Health care providers who fail to provide an itemized statement may be subject to a CMP of not more than $100 for each failure to furnish the information (§1806(b)(2)(B) of the Social Security Act). An itemized statement is defined as a listing of each service(s) or item(s) provided to the beneficiary. Statements that reflect a grouping of services or items (such as a revenue code) are not considered an itemized statement.

A beneficiary who files a complaint with a MAC regarding a provider’s failure to provide an itemized statement must initially validate that his/her request was in writing (if available), and that the statutory 30-day time limit (calendar days) for receiving the information has expired. In most cases, an additional 5 calendar days should be allowed for the provider to receive the beneficiary’s written request. If the beneficiary did not make his/her request in writing, inform him/her that he/she must first initiate the request to the provider in writing. It is only after this condition and the time limit condition are met that the MAC may contact the provider.

Once the MAC confirms that the complaint is valid, the MAC shall initiate steps to assist the beneficiary in getting the provider to furnish the itemized statement. MACs shall initiate the same or similar procedures when receiving complaints regarding mandatory submission of claims (i.e., communicating with the provider about their non-compliance and the possibility of the imposition of a CMP).

If the intervention of the MAC results in the provider furnishing an itemized statement to the beneficiary, the conditions for the statute are considered met, and a CMP case should not be developed. Should the intervention of the MAC prove unsuccessful, the MAC shall consider referral to the *UPIC* for subsequent referral of the potential CMP case to CMS, following the guidelines established in PIM Chapter 4, §§4.20.3.1 and 4.20.4. There may be instances where a beneficiary receives an itemized statement and the MAC receives the beneficiary's request (written or oral) to review discrepancies on his/her itemized statement. MACs shall follow their normal operating procedures in handling these complaints. MACs shall determine whether itemized services or items were provided, or if any other irregularity (including duplicate billing) resulted in improper Medicare payments. If so, the MAC shall recover the improper payments.

4.21 - Monitor Compliance

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

The *UPIC* shall monitor future claims and related actions of the provider at least 6 months after the *UPIC* has closed its investigation to ensure the propriety of future payments. In addition to internal screening of the claims, if previous experience or future billings warrant, they shall periodically interview a sampling of the provider's patients to verify that billed services were actually furnished.
If, at the end of a 6-month period, there is no indication of a continuing aberrant pattern, the *UPIC* shall discontinue the monitoring.

4.21.1 - Resumption of Payment to a Provider - Continued Surveillance After Detection of Fraud

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

After completion of the investigation and appropriate legal action, all determined overpayments are recouped by either direct refund or offset against payments being held in suspense. Once recoupment is completed, *UPICs* shall release any suspended monies that are not needed to recoup determined overpayments and, if applicable, penalties.

UPICs shall monitor future claims and related actions of the provider for at least 6 months, to assure the propriety of future payments. In addition to internal screening of the claims, if previous experience or future billings warrant, they shall periodically interview a sampling of the provider's patients to verify that billed services were actually furnished.
If, at the end of a 6-month period, there is no indication of a continuing aberrant pattern, *UPICs* shall discontinue the monitoring.

4.22 - Discounts, Rebates, and Other Reductions in Price

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

A *UPIC* that learns of a questionable discount program shall contact *its IAG BFL to determine the course of action, when needed.*

4.22.1.1 - Marketing to Medicare Beneficiaries

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

Certain marketing or solicitation practices could be in violation of the Medicare anti-kickback statute, 42 U.S.C. 1320a-7b(b). All marketing practices shall comply with the Medicare anti-kickback statute and with the Office of the Inspector General's (OIG's) Compliance Program Guidance for the DMEPOS industry.

Marketing practices may influence Medicare beneficiaries who use medical supplies, such as blood glucose strips, on a repeated basis. Beneficiaries are advised to report any instances of fraudulent or abusive

practices, such as misleading advertising and excessive or non-requested deliveries of test strips, to their durable medical equipment MACs.

Advertising incentives that indicate or imply a routine waiver of coinsurance or deductibles could be in violation of 42 U.S.C. 1320a-7b(b). Routine waivers of coinsurance or deductibles are unlawful because they could result in--1) false claims; 2) violation of the anti-kickback statute; and/or 3) excessive utilization of items and services paid for by Medicare.
In addition, 42 U.S.C. 1320a-7a(a) (5) prohibits a person from offering or transferring remuneration. Remuneration is a waiver of coinsurance and deductible amounts, with exceptions for certain financial hardship waivers that are not prohibited.

Suppliers should seek legal counsel if they have any questions or concerns regarding waivers of deductibles and/or coinsurance or the propriety of marketing or advertising material.
Any supplier that routinely waives co-payments or deductibles can be criminally prosecuted and excluded from participating in Federal health care programs.

4.22.2 - Cost-Based Payment (Intermediary and MAC Processing of Part A Claims): Necessary Factors for Protected Discounts

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This applies to *UPIC*s and MACs.

For a discount to be protected, certain factors must exist. These factors assure that the benefit of the discount or rebate will be reported and passed on to the programs. If the buyer is a Part A provider, it must fully and accurately report the discount in its cost report. The buyer may note the submitted charge for the item or service on the cost report as a "net discount." In addition, the discount must be based on purchases of goods or services bought within the same fiscal year. However, the buyer may claim the benefit of a discount in the fiscal year in which the discount is earned, or in the following fiscal year. The buyer is obligated, upon request by the HHS or a state agency, to provide information given by the seller relating to the discount.

The following types of discounts may be protected if they comply with all of the applicable standards in the discount safe harbor:

- Rebate check
- Credit or coupon directly redeemable from the seller
- Volume discount or rebate

The following types of discounts are not protected:

- Cash payment
- Furnishing one good or service free of charge or at a reduced charge in exchange for any agreement to buy a different good or service
- Reduction in price applicable to one payer but not to Medicare or a State health care program
- Routine reduction or waiver of any coinsurance or deductible amount owed by a program beneficiary

Note: There is a separate safe harbor for routine waiver of co-payments for inpatient hospital services. (Refer to 42 CFR §1001.952(k)(1).)

4.22.3 - Charge-Based Payment (MAC Processing of Part B Claims): Necessary Factors for Protected Discounts

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s and MACs.

For a discount program to be protected for Part B billing, certain factors must exist. These factors ensure that the benefit of the discount or other reduction in price is reported and passed on to the Medicare or Medicaid

programs. A rebate rendered after the time of sale is not protected under any circumstances. The discount must be made at the time of sale of the good or service. In other words, rebates are not permitted for items or services if payable on the basis of charges. The discount must be offered for the same item or service that is being purchased or furnished. The discount must be clearly and accurately reported on the claim form.

The following types of discounts may be protected if they comply with all of the applicable standards in the discount safe harbor:

Credit or coupon directly redeemable from the seller

The following types of discounts are not protected:

• Rebates offered to beneficiaries

• Cash payment

• Furnishing an item or service free of charge or at a reduced charge in exchange for any agreement to buy a different item or service

• Reduction in price applicable to one payer but not to Medicare or a State health care program

• Routine reduction or waiver of any coinsurance or deductible amount owed by a program beneficiary

NOTE: There is a separate safe harbor for routine waiver of co-payments for inpatient hospital services. (Refer to 42 CFR §1001.952(k)(1).)

4.22.4 - Risk-Based Provider Payment: Necessary Factors for Protected Discounts

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

If the buyer is a health maintenance organization or a competitive medical plan acting in accordance with a risk contract or under another state health care program, the buyer does not need to report the discount, except as otherwise required under the risk contract.

4.23 - Identity Theft – Physicians

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s.

*UPIC*s shall conduct investigations of potential fraud, waste, or abuse of physician identities. An example of physician identity theft may include a physician's identity having been stolen and used to establish a new billing number (reassignment), causing inappropriate Medicare payments to unknown person(s) and potential Internal Revenue Service (IRS) issues for the victimized physician.

The *UPIC* shall discuss the identity theft case with the COR and IAG BFL. If claims are still being submitted and Medicare payments are being made, consider requesting a prepayment review, auto-denial edit, or immediate payment suspension.

The IAG BFL will determine if the physician will be treated as a victim of identity theft and will coordinate the referral of correcting the inaccurate information to the appropriate CMS component.

The *UPIC* shall provide the following information to the COR and IAG BFL, if appropriate:

- Name, fraudulent address, ID number, and tax identification number (TIN).
- Name, correct address, ID number, and TIN.
- A signed attestation from the physician indicating that there was no knowledge that identity information was stolen and used to establish a Medicare billing number.
- Furthermore, the physician attests that he/she did not receive any of the potential fraudulent reimbursements, either directly or indirectly.
- A brief summary of how the fraud occurred and was discovered.
- The total dollars paid (by calendar year) under the fraudulent number.
- Name of MAC involved.
- Amount of money that has been recovered by the MAC.
- *Any law enforcement and/or court documents which are relevant to the determination of the alleged identity theft.*

The amount of money seized and being held by law enforcement

4.28 - Joint Operating Agreement

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s, MACs, RA*C*s, and QICs, as indicated.

A Joint Operating Agreement (JOA) is a document developed between two entities (CMS contractors) that delineates the roles and responsibilities of each entity regarding their interactions with each other on CMS contracts.

*UPIC*s shall have JOAs with the following *entities*:

- QICs (refer to PIM Exhibit 45 for a sample JOA between the *UPIC* and the QIC)
- RA*C*s (refer to PIM Exhibit 44 for a sample JOA between the UPIC and the RA*C*)
- State agencies (refer to the UPIC USOW and the Medicaid Policies and Procedures Manual *(PPM), which is an appendix of the UPIC USOW*).
- MACs
- Pricing, Data Analysis, and Coding Contractor (PDAC)
- *National Supplier Clearinghouse (*NSC*)*
- National Benefit Integrity Medicare Drug Integrity Contractor

As it applies to the *UPIC*'s task orders, the JOA with the MACs shall, at a minimum, provide information on assigned responsibilities, timeframes, processes and procedures, and coordination. *Additional detail related to this information is referenced in the UPIC USOW.*

Periodically, there are instances where the UPIC is in need of the requested information in a shorter timeframe than (30) calendar days. To account for these instances, the UPIC and MAC may add language to their Joint Operating Agreement that allows for a shorter timeframe for the MAC to furnish the requested information (i.e. 48 hours, 72, hours, etc.).

4.31 – Vulnerabilities

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s *& MEDIC*.

Program vulnerabilities are identified flaws or weaknesses in policy and/or regulatory authority that increases the likelihood of significant inappropriate payments being made to a broad provider/supplier population. Program vulnerabilities can be identified through a variety of sources such as the chief financial officer's (CFO) audit, Fraud Alerts, the Government Accountability Office (GAO), the Office of Inspector General (OIG), data driven studies, and *UPIC* and Medicare contractor operations, as examples.

Program Integrity Concerns are issues CPI and/or the UPICs/MEDIC have identified through their own analysis and have the ability to mitigate through existing operations. Examples of Program Integrity Concerns include, but are not limited to: routine changes and implementation of new billing codes (i.e. ICD-10, HCPCs, CPT codes, etc.) that may lead to questionable billing practices, reports/complaints of a potential fraud schemes that can be addressed in CMS regulations or policy guidance, or identified concerns and significant mitigating changes to enrollment processes.

The UPICs & MEDIC shall discuss potential Program Vulnerabilities with the COR(s) and BFL(s) during the established recurring workload meetings. Program Vulnerabilities should be submitted sooner if the UPIC/MEDIC believes it requires immediate consideration. The BFL will validate the lead to determine whether the potential issue is a Program Vulnerability, a Program Integrity Concern, or another type of issue that may need to be addressed. Should the BFL need additional information, the UPIC/MEDIC shall submit an overview of potential Program Vulnerability, program impact, and proposed action to the COR(s) and BFL(s) via email.

Should the COR(s) and BFL(s) agree that the identified issue is a Program Vulnerability, the UPIC/MEDIC shall submit the proposed Program Vulnerability to the vulnerability mailbox at CPIVulnerabilityIntake@cms.hhs.gov, using the Vulnerability Template. Additionally, all Program Vulnerabilities that are submitted to the mailbox shall be documented in the UPIC/MEDIC program vulnerability report. If the UPIC/MEDIC believes the proposed Program Vulnerability has potential Medicaid impact, the UPIC/MEDIC shall document this in the submission to the vulnerability mailbox.

Should the COR(s) and BFL(s) determine that the identified issue is a Program Integrity Concern, the COR(s) and BFL(s) shall advise the UPIC/MEDIC to mitigate the concern through their existing operations. Issues not considered to be Program Vulnerabilities or Program Integrity Concerns will be addressed on a case by case basis.

Vulnerability Template

Date Submitted:

Submitted by

Name: Organization:
Phone: Email:

Vulnerability Vulnerability Name:

Description: Proposed Action:

Source (i.e. person/organization that first identified it): FPS Model-

Related (Y/N):

* If yes, simultaneously report the information consistent with requirements of the FPS.

List Attachments:

4.33 – *UPIC* Coordination with *Other Contractors Related to the RAC Data Warehouse*

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPIC*s, RA*C*s, *MACs, and SMRC* as indicated.

The CMS established the RA*C* Data Warehouse *(RACDW)* to track RA*C* activity and prevent conflicts between RA*C* reviews and other program integrity activities. The success of this mission depends on timely and accurate information reporting by the *UPIC*s, as well as by claims processing contractors and by the RA*C*s themselves. *CMS has expanded the functionality of the RACDW to allow all contractors that perform medical review to collaborate so there is no duplication of effort.*

To prevent *other contractors from* interference with active investigations or cases, *UPIC*s shall enter suppressions in the RA*C* Data Warehouse to temporarily mark entire providers/suppliers or subsets of a provider's/supplier's claims as "off-limits" to the RA*C*s*, MACs, and SMRC. The suppression must be entered in the RACDW when the investigation is opened, but no later than 2 business days after the investigation is opened*.

Individual claims that have been previously reviewed (or that are part of an extrapolated settlement universe) shall be excluded to permanently block them from repeat reviews by a RA*C, MAC or SMRC*.

The RA*C* Data Warehouse allows users to enter suppressions on any combination of provider ID, Diagnostic Related Group (DRG), International Classification of Diseases-9/10 (ICD-9/10) procedure code, Healthcare Common Procedure Coding System (HCPCS) code, State, or ZIP code although CMS requires that suppressions be tailored as narrowly as possible. *UPIC*s shall suppress targeted procedure codes from specific providers/suppliers associated with open investigations/cases. Suppressions of one or more procedure codes across an entire geographic area may be considered in egregious situations of widespread fraud*, waste* and*/or* abuse of specific codes or types of services (e.g., infusion therapy in South Florida).

The Data Warehouse can accept suppressions on a rendering provider, supplier, or institution ID. Suppressions on referring, ordering, billing (for professional DME claims) and attending providers (institutional claims) are not currently supported.

Whether suppressing an entire provider or only a portion of a provider's claims, the *UPIC* shall indicate the nature of the provider being suppressed (i.e., hospital, individual physician, physician group, home health agency, etc.) in the provider type field, using the codes specified in the Data Warehouse. The *UPIC* shall also indicate the name of the provider being suppressed in the comment field, which can accommodate up to 256 characters.

When entering a suppression on a six-digit provider/supplier ID, the *UPIC* shall also enter the provider's/supplier's practice State. States are not required for NPIs, NSC numbers, alphanumeric or PTANs that are other than six digits long; but six-digit PTANs potentially overlap with six-digit CMS institutional provider numbers. Having the provider/supplier state will help CMS suppression reviewers to differentiate among multiple providers/suppliers with the same ID.

Specific suppression start and end dates are also mandatory. Suppressions can extend up to three (3) years into the past and one (1) year forward from date of entry (the start date is initially fixed at 10/1/2007, which is the earliest start date that RACs can select for their reviews). Users will be notified as their suppressions approach the expiration dates and can renew them if necessary. CMS expects users to release them sooner if the underlying investigations/cases are closed.
Once a suppression is lifted or expires, *UPIC*s are also responsible for entering any necessary exclusions. Any claims for which the *UPIC* has requested medical records shall be excluded to prevent re-review by a

RA*C*, unless the *UPIC*'s review resulted in a full denial. In this case, exclusion is unnecessary because the provider/supplier will either appeal and the redetermination entity will enter the exclusion, or the provider/supplier will allow the decision to stand. The exclusion will be unnecessary because the RA*C*s are unlikely to pursue zero-dollar claims).

In addition, the UPICs shall review the RACDW to determine if other contractors currently have a particular provider under review. If the provider is under review by another contractor (RAC, MAC, SMRC) the UPIC shall contact that respective contractor to determine which entity should continue to review that provider and how to handle the current medical review, i.e. close it out or complete the medical review and then refer to the UPIC.

Below are examples of suppressions and exclusions in various circumstances: this list is not all-inclusive. The *UPIC* staff may need to consult with its respective CMS COR and BFLs and/or CMS RA*C* liaison to determine the appropriate level of suppression or exclusion.

4.34 - Suppression and/or Exclusion – Examples

(Rev. 851, Issued: 12-14-18, Effective: 10-22-18, Implementation: 10-22-18)

This section applies to *UPICs* and RA*C*s, as indicated.

• Suppressions of providers/suppliers that the *UPIC* has referred to law enforcement and are the subject of a law enforcement investigation should remain effective until the provider's/supplier's case is returned with a declination for prosecution from law enforcement and without a request for *UPIC* administrative action. The suppression may be entered using one of the following methods:

Suppression at the provider/supplier and/or geographic level requires the user to supply detailed justification for each request; in addition to provider name/type, *NPI,* start/end dates, *CSE number,* and other fields as specified in the RA*C* Data Warehouse User's Guide. *UPIC*s shall routinely monitor accepted suppression records to ensure that the suppressions remain relevant/appropriate and that they are ultimately released in a timely manner.

Suppression at the procedure code level for individual providers/suppliers may be done without providing justification, due to the narrower scope of the suppression. Suppressions at this level still require the user to supply a DRG, ICD-9/10 procedure or HCPCS code, provider/supplier identifiers, *NPI,* start and end dates, *CSE number,* and any additional information as defined in the RA*C* Data Warehouse User's Guide.

Note: The RA*C*s can review claims paid as early as 10/1/2007, which is before NPI submission became mandatory. Therefore, *UPICs* are strongly encouraged to enter suppressions on both NPIs and legacy provider/supplier numbers for suppressions that cover the period of October 2007 through May 2008.

Suppression/Exclusion for postpayment review where extrapolation may or may not be performed – In the event that the *UPIC* is unable to determine at the time of review whether any overpayments that are identified will be extrapolated to the parent claim universe, the *UPIC* shall enter a suppression on the relevant provider/supplier ID and service code(s). If the *UPIC* does ultimately assess an extrapolated overpayment, the *UPIC* shall release the suppression and exclude the entire universe. If the overpayment is computed based only on the sampled claims (i.e., the overpayment is not projected to the entire universe), the *UPIC* shall release the suppression and exclude only the sample claims that were actually reviewed.

Exclusion for prepayment edits or clinically unlikely edits (CUEs) – Claims that have been subjected to automated edits only are still eligible for RA*C* review and should generally not be excluded. Claims that have subsequently undergone *medical record* review do require exclusion.
Exclusion for prepayment review – In those instances in which a provider/supplier is under investigation and is subject to 100% prepayment review, a suppression will not be necessary because the RA*C*s do not receive claim data in real time. However, all individual claims that were reviewed shall be excluded (this

requirement applies whether the provider/supplier was on 100% prepayment review, or a lesser fraction of that provider's/supplier's claims were being reviewed).

For access to the RA*C* Data Warehouse, contact the system administrators at rac@cms.hhs.gov. Current suppression/exclusion file layouts and the user's guide are available from the help desk staff or by download from the system itself.

The *UPICs* shall have a JOA with the RA*C*s. Refer to PIM Exhibit 44 for the JOA between the *UPICs* and the RA*C*s. The *UPICs* shall include in the JOA quarterly meetings with the RA*C* in their zone, at a minimum, to discuss trends in possible fraudulent billing. If *UPICs* or RA*C*s have any recommendations for modifying the JOA, they shall provide these modifications to their respective CORs.