CMS Manual System	Department of Health & Human Services (DHHS)
Pub 100-08 Medicare Program Integrity	Centers for Medicare & Medicaid Services (CMS)
Transmittal 10711	**Date: April 1, 2021**
	Change Request 12135

Transmittal 10641, dated March 18, 2021, is being rescinded and replaced by Transmittal 10711, dated April 1, 2021, to remove the revision to section 4.6.2, Chapter 4 of Pub. 100-08, and update the revision to section 4.6.3, Chapter 4 of Pub. 100-08. All other information in this transmittal 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 in Pub. 100-08.

EFFECTIVE DATE: April 19, 2021
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: April 19, 2021

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	4/4.2/4.2.2.1/Organizational Requirements
R	4/4.2/4.2.2.4/Procedural Requirements
R	4/4.2/4.2.2.6/Program Integrity Security Requirements
R	4/4.4/4.4.1/Requests for Information From Outside Organizations
R	4/4.6/4.6.3/Screening Leads
R	4/4.6/4.6.4/Vetting Leads with CMS
R	4/4.7/4.7.1/Conducting Investigations
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	4/4.9/4.9.3/Guidelines for Incentive Reward Program Complaint Tracking
R	4/4.10/Fraud Alerts
R	4/4.13/Administrative Relief from Program Integrity Review in the Presence of a Disaster
R	4/4.17/UPIC Hospice Cap Liability Process – Coordination with the MAC
R	4/4.18/4.18.1/Referral of Cases to the OIG/OI
R	4/4.18/4.18.1.2/Immediate Advisements to the OIG/OI
R	4/4.18/4.18.1.5/Referral to Other Law Enforcement Agencies
R	4/4.18/4.18.1.5.3/Reserved for Future Use
R	4/4.18/4.18.2/Referral to State Agencies or Other Organizations
R	4/4.18/4.18.3/UPICs and QIOs
R	4/4.22/Discounts, Rebates, and Other Reductions in Price
R	4/4.23/Identity Theft Investigations and Victimized Provider Waiver of Liability Process

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: 107011	Date: April 1, 2021	Change Request: 12135

Transmittal 10641, dated March 18, 2021, is being rescinded and replaced by Transmittal 10711, dated April 1, 2021, to remove the revision to section 4.6.2, Chapter 4 of Pub. 100-08, and update the revision to section 4.6.3, Chapter 4 of Pub. 100-08. All other information in this transmittal remains the same.

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

EFFECTIVE DATE: April 19, 2021
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: April 19, 2021

I. GENERAL INFORMATION

A. Background: The CMS will make revisions to Chapter 4 in Pub. 100-08 based on updates to Unified Program Integrity Contractor (UPIC) and Investigations Medicare Drug Integrity Contractor (I-MEDIC) processes.

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

II. BUSINESS REQUIREMENTS TABLE

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

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
12135.1	Contractors shall be aware that all references to Investigations and Audits Group and IAG have been removed from Chapter 4 in Pub. 100-08.									UPICs
12135.2	The UPIC shall include policy / regulation analysis in their lead screening									UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	process.									
12135.3	The UPICs shall submit requests for any investigative activities that require approval by CMS through its current processes and coordinate subsequent actions with the appropriate points of contact within the Center for Program Integrity.									UPICs
12135.4	The UPICs shall coordinate with the MAC to determine whether a hospice is subject to any finalized or ongoing cap liability reviews for the applicable period of the UPIC's audit when selecting claims using statistical sampling that may result in an actual and/or extrapolated overpayment.									UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
12135.4.1	The UPICs shall proceed with its medical review if there are no cap liability determinations.									UPICs
12135.4.1.1	The UPIC shall coordinate with the MAC, upon identifying an overpayment, to ascertain whether in the intervening period (from the claims selection period to the overpayment determination) as to whether the hospice had become subject to any cap liability proceedings for that same period.									UPICs
12135.4.2	The UPIC shall finalize its review, issue the findings to the hospice, and refer any overpayment to the MAC for collection.									UPICs
12135.4.2.1	The MAC shall take into account the			X						

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	cap liability and adjust as appropriate.									
12135.4.3	The UPIC shall consult with the MAC and design a statistical sampling for overpayment estimation for those specific year(s) according to the cap determinations to assist with reconciling cap overpayments if it is determined that the hospice is subject to any finalized or ongoing cap liability reviews.									UPICs
12135.4.3.1	The UPIC shall finalize its review and issue the findings to the hospice and refer any overpayment to the MAC.									UPICs
12135.4.3.2	The MAC shall take into account the overpayments submitted by the UPIC and apply these to any			X						

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	subsequent, ongoing cap overpayments.									
12135.5	The UPICs shall provide the Office of Inspector General (OIG) / Office of Investigations (OI) with all available documentation, including billed/paid amounts for the YTD and the previous year, if the OIG/OI confirms that a formal immediate advisement should be sent.									UPICs
12135.5.1	The UPICs shall notify the CMS identified Strike Force points of contacts if providers and/or suppliers within an immediate advisement notification are located within a Strike Force jurisdiction.									UPICs
12135.6	The UPICs shall adhere to the guidance									UPICs

Number	Requirement	Responsibility								
		A/B MAC			DME MAC	Shared-System Maintainers				Other
		A	B	HHH		FISS	MCS	VMS	CWF	
	as outlined in section 4.18.1.5, Chapter 4 of Pub. 100-08, when making referrals to other law enforcement agencies.									

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. 10711; Issued: 04-01-21)

Transmittals for Chapter 4

4.2.2.1 Organizational Requirements

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

This section applies to UPICs 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 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.

4.2.2.4 - Procedural Requirements

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

This section applies to UPICs 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 which the referral was made.

The MAC shall provide written procedures for personnel in various contractor functions (claims processing, MR, beneficiary services, 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 the UPICs 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) and;

- 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, UPICs, 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 UCM, provide ideas and feedback on Fraud Alerts and/or vulnerabilities within the Medicare or Medicaid programs;

- Report to the Contracting Officer's Representative (COR) and the Business Function Lead (BFL) all situations that have been identified in which a provider consistently fails to comply with the provisions of the assignment agreement; and

- Coordinate and communicate with the MR units within the MACs to avoid duplication of work.

Coordination with 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 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 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 in which their personal safety is in question; and

- Maintain independence from LE and do not collect evidence, i.e., request medical records or conduct interviews, at LE's 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 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, state MFCUs);

- Help to develop fraud-related outreach materials (e.g., pamphlets, brochures, videos) in cooperation with beneficiary services and/or provider relations department of the MACs for use in their training. Submit written outreach material to the COR and 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 BFLs; and

- 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 in which 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); and

- Ensure no payments are made to a Medicare provider/supplier that employs an excluded individual or entity.

4.2.2.6 - Program Integrity Security Requirements

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

This section applies to UPICs.

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 UPICs collect in administering UPIC contracts belong to CMS. Thus, the UPICs 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 UPICs 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 UPICs all local workstations as well as workstations used at home by UPICs 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 UPICs shall require existing employees to complete a conflict of interest declaration, as well as a confidentiality statement.

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

At least once a year, the UPICs 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 UPICs 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 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 UPICs shall implement phone security practices. The UPICs 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 UPICs 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 UPICs 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, UPICs shall not respond to questions concerning any case the OIG, the FBI, or any other LE agency is investigating. The UPICs shall refer such questions to the OIG, the FBI, etc., as appropriate.

Finally, the UPICs 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, UPICs shall make arrangements with the addressee to have someone waiting at the receiving machine while the fax is transmitting. The UPICs 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.

4.4.1 - Requests for Information From Outside Organizations

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

This section applies to UPICs.

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 UPICs;
- Qualified Independent Contractors (QICs);
- QIOs;
- State Attorneys General and State Agencies;
- MFCUs;
- OIG;
- DOJ; and
- FBI.

Requests for information from entities not listed above shall be submitted to the COR for approval, with a copy to the 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 /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, UPICs 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 U.S. 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 UPICs 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 systems of record, and a decision concerning the applicability of a routine use lies solely in the purview of the system's manager for each system of record. 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 U.S. 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 UPICs shall refer requests that raise Privacy Act concerns and/or issues to the CORs for further consideration.

A. Requests from Private, Non-LE Agencies

Generally, UPICs may furnish information on a scheme (e.g., where it is operating or 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 BFL for further guidance.

B. Requests from Other UPICs

The UPICs may furnish requested specific information concerning ongoing fraud investigations and individually identifiable PHI to any UPIC, SMRC or MAC. The UPICs, SMRCs 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 RFI received from another UPIC and notify the requesting UPIC that the case has been referred to the OIG/OI.

C. RFI from QICs

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 QIOs 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, UPICs 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 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 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 MFCUs

Under current Privacy Act requirements applicable to PI 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. An RFI shall consist of requests to run data for the OIG (including OnePI national data for suppliers and entities whose billed claims span across multiple jurisdictions), 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 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 in which 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 (JOA) 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, 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 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. An RFI 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 UPICs 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 (RFA) – An LE RFA is a type of RFI 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) the 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.

The 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 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 it subsequently anticipates 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 DOJ

In April 1994, CMS entered into an interagency agreement with the OIG and the DOJ that permitted UPICs 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 U.S. Attorneys, 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 UPIC shall provide the DOJ with the requested information and shall maintain cost information related to fulfilling these requests. An RFI shall consist of requests to run data for the DOJ (including national data for suppliers and entities whose claims billings span across multiple jurisdictions), extract of records, or a request to furnish any documentation or reports.

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 25).

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 RFI 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 in which 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 JOA 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. An RFI 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 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.

RFA – A LE RFA is a type of RFI 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.

The 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 PI 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 it subsequently anticipates 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 RFIs

If the UPIC receives duplicate or similar RFIs 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 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; and
- The date completed.

K. LE Requests for MR

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 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 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. LE 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 BFL. The UPIC shall provide its COR and copy its 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 timeframe and cost agreed upon with LE.

M. Requests from LE for Information Crossing Several UPIC Jurisdictions

If a UPIC receives a RFI from LE that crosses several UPIC zones, the UPIC shall contact its COR and BFL. In the event that multiple zones are providing information in connection with the request, each UPIC shall enter a separate entry into the UCM as described in Section 4.12 of this chapter. The COR and BFL may assign a lead UPIC to process these requests that will coordinate with the other UPICs to obtain the necessary data and consolidate the information into one comprehensive response for the requestor. The lead UPIC may be the UPIC that initially received the request; however, the nature of the RFI should be considered when assigning a lead UPIC.

4.6.3 - Screening Leads

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

This section applies to UPICs.

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 45 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;
- Coordination with the MAC on prior activities (i.e., prior medical reviews, education, appeals information, etc.);
- Data analysis;
- *Policy / regulation analysis;*
- Contact with the complainant, when the lead source is a complaint;
- Beneficiary interviews; 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 UCM that would raise additional concerns, the UPIC shall contact its COR and 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 45 calendar days, the UPIC shall document the reasons, circumstances, dates, and actions associated with the delay to its COR and BFL within its monthly reporting in CMS ARTS.

If the UPIC identifies specific concerns while screening a lead that warrants contact with a specific provider/supplier, the UPIC shall contact its Contract Office Representative (COR) and Business Function Lead (BFL) for further guidance (e.g., UPIC determines that provider/supplier contact is needed in order to determine if the case warrants further investigation).

4.6.4 - Vetting Leads with CMS

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

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 National Provider Identifiers (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. Periodically, based on high priority fraud schemes identified by CMS and/or Law Enforcement, CMS may require the UPIC to vet leads in an expedited timeframe. When instances such as this are identified, the details associated with the expedited vetting will be communicated to the UPIC by their COR and BFL.

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 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 UPIC shall complete the appropriate updates in the UCM 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).

4.7.1 - Conducting Investigations

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

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

- Screening activities as referenced in Section 4.6.3;
- Contact with the subject provider or ordering/referring providers via telephone or on-site visit;

- Medical record requests and reviews (as defined in PIM, chapter 3);
- Prepayment medical reviews associated with a limited claim count (i.e., 25- 50 claims) or targeted review (i.e., specific CPT codes) (as defined in PIM, chapter 3);
- Implementation of auto-denial edits; and
- Recommendation of other administrative actions (as defined in PIM chapters 3, 8, and 15) to CMS. These items will include any administrative actions identified below to be discussed during the case coordination meetings.

Additionally, the UPICs shall coordinate with LE partners prior to making contact with any provider/supplier, when it knows there is or was a LE case on the provider/supplier. The UPIC shall review the Unified Case Management (UCM) system prior to contacting any provider/supplier to verify the following:

- There are no current or prior requests for information from LE;
- There are no other current or prior coordination activities with LE concerning the provider; and
- The CMS vetting response indicates there is no current LE activity associated with the provider/supplier.

If the UPIC identifies prior LE activity within the past 24 months, the UPIC shall communicate with the LE contact person identified in the UCM to determine if making contact with a provider/supplier will impact its case. If the UPIC is not able to identify the LE contact person in UCM, the UPIC shall consult with its BFL for further guidance. Once the UPIC contacts LE, it shall document the results of the conversation, including the date, time, name of the individual, and the specific LE agency in UCM prior to contacting the provider/supplier. If the UPIC has attempted to contact LE on multiple occasions within five (5) business days, but does not receive a response, the UPIC shall notify its COR and BFL for CMS escalation to the appropriate LE contacts.

For any investigative activities that require approval by CMS (i.e., Payment Suspension, Requests for Anticipated Payment (RAP) suppression, or revocation/deactivation requests), the UPIC shall submit those requests through its current processes (i.e., via UCM) and coordinate subsequent actions with the appropriate points of contact within *CPI*.

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 BFL approval prior to initiating the overpayment.

4.8.1 - Reversed Denials by Administrative Law Judges on Open Cases

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

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. UPICs 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 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. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

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, UPICs 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. UPICs 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. UPICs 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 BFL immediately.

4.9.3 - Guidelines for Incentive Reward Program Complaint Tracking

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

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

4.10 - Fraud Alerts

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

This section applies to UPICs.

Fraud Alerts are issued when circumstances arise that indicate a need to advise the UPICs, SMRCs, MACs, LE, 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 BFL a summary of the circumstances. The 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 UPICs in the UCM. Once the information is disseminated, the UPIC may send any questions related to the Fraud Alert to the COR and BFL.

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

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

This applies to the UPICs.

The UPICs shall be aware of Federal Emergency Management Agency (FEMA) declared natural disasters that occur in their jurisdiction(s). In the immediate aftermath of these occurrences, the UPICs shall assess the circumstances with each provider in declared disaster areas before pursuing investigative activities.

Due to the nature of fraud, waste and abuse that exists in the Medicare program and the potential for emerging trends specific to FEMA declared natural disasters, contractors should remain vigilant in their oversight, monitoring, and proactive/reactive analysis but follow the guidance identified below:

1) Should the contractor confirm that medical record loss resulted from this disaster to the point where administrative relief from medical review requirements is necessary to allow the provider sufficient time to retrieve copies of, or restore damaged, medical documentation, the contractors shall delay the request for medical records for a period of 60-days beginning on the date designated by FEMA/as advised by COR/BFL and ending as directed by their COR/BFL. The contractors are permitted to respond to inquiries, requests, or complaints that are submitted by a provider or beneficiary during this 60-day period;

2) The contractors shall consult with their COR and BFL on any time sensitive issues that must be resolved involving contact with a provider or beneficiary in the areas affected by FEMA declared natural disasters;

3) The contractors shall closely monitor Technical Direction Letters (TDLs) and Change Requests (CRs) issued to the MACs related to FEMA designated disaster relief efforts. The contractors shall consult with the COR and BFL on any questions resulting from MAC TDLs or CRs; and

4) The contractors are reminded to contact their COR and BFL prior to granting specific relief based on any TDL guidance or PIM requirement. Each contractor shall maintain a list of cases/investigations/complaints to which any exception is granted or applied and must include the basis (TDL or PIM reference) and the actual exception applied.

During a governmentally declared disaster, whether manmade or otherwise, the UPIC shall continue every effort to identify cases of potential fraud, waste, and abuse. 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 in which backup records exist, the UPIC shall accept reproduced medical records from microfiche, microfilm, 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 in which no backup records exist, the UPICs shall consult with its COR and BFL to determine the appropriateness of the request to reconstruct the medical records. If the COR and BFL determine that MR 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."

4.17 - UPIC Hospice Cap Liability Process – Coordination with the MAC

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

This section applies to UPICs.

Medicare Part A includes a hospice benefit for terminally ill patients. Congress has established a retrospective "cap" on the aggregate amount that Medicare will reimburse hospice providers each year. Historically, PI contractor reviews of hospices have overlapped with the MAC review of the benefit cap liability for those same hospices; resulting in a potential double recovery for the government. Therefore, the following communication and process between the UPICs and MACs shall be followed, in order to minimize the occurrence of these double recoveries, and check the RAC Data Warehouse to ensure the provider is not under suppression.

- UPIC Initiated Reviews:

    - *When selecting claims using statistical sampling that may result in an actual and/or extrapolated overpayment, upon the initiation of a hospice review, the UPIC shall coordinate with the MAC to determine whether the hospice is subject to any finalized or ongoing cap liability reviews (self-reported, final, and/or re-opening) for the applicable period of the UPIC's audit.*

      If there are no cap liability determinations, the UPIC shall proceed with its review. Upon identification of an overpayment, the UPIC shall coordinate with the MAC to ascertain whether in the intervening period (from the claims selection period to the overpayment determination) the hospice had become subject to any cap liability proceedings for that same period.

      The UPIC shall finalize its review and issue the findings to the hospice and refer any overpayment to the MAC for collection. The MAC shall take into account the cap liability and adjust as appropriate.

      If it is determined that the hospice is subject to any finalized or ongoing cap liability reviews (self-reported, final, and/or re-opening), the UPIC shall consult with the MAC and design a statistical sampling for overpayment estimation (SSOE) for those specific year(s) according to the cap determinations to assist with reconciling cap overpayments. The UPIC shall finalize its review and issue the findings to the hospice and refer any overpayment to the MAC. The MAC shall take into account the overpayments submitted by the UPIC and apply these to any subsequent, ongoing cap overpayments (self-reported, final, and/or reopening). This process ensures

that a provider is not penalized for the same beneficiary twice.

4.18.1 - Referral of Cases to the OIG/OI

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

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. 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.

If the UPIC believes a case should be referred to LE, the UPIC shall discuss the matter with its BFL. If the BFL agrees that referral to LE is appropriate, the UPIC shall update the UCM appropriately to ensure the provider/supplier is included in the next case coordination meeting discussion for final approval. If it is determined an investigation should be referred to LE, the UPIC shall refer the matter to the designated OIG/OI Special Agents-in-Charge (SAC), Department of Justice Assistant United States Trial Attorneys, or other parties identified during the case coordination discussion. In such instances, the UPIC shall make immediate referrals to the designated parties within seven (7) calendar days, unless otherwise specified by its COR and BFL.

Referrals to LE shall include all applicable information that the UPIC has obtained through its investigation at the time of the referral. The UPIC shall utilize the "LE Referral Template" available in PIM Exhibit 16.1 Additionally, if the referral is related to a multi-jurisdiction or national provider/supplier, the UPIC shall coordinate and collect all applicable investigative information from the other UPICs that have an open investigation on that same provider/supplier. The UPIC shall then send one comprehensive referral with all the UPICs' investigative findings to LE. Once the referral package is complete, the UPIC shall submit the referral to LE and copy its COR and BFL. Upon submission of the referral to LE, the UPIC shall request written and/or email confirmation from LE acknowledging receipt of the referral. UCM shall be updated with the date the referral was sent, the name of the agent acknowledging receipt of the referral, and the date of receipt. In the event that written confirmation is not received, the UPIC shall notify the COR and BFL.

As previously instructed, the UPIC shall continue to refrain from implementing any additional administrative actions against the provider/supplier without CMS approval during the 60-day window OIG/OI and/or DOJ has to respond to the referral. If the UPIC has any questions related to referrals, the UPIC shall coordinate with its COR and BFL.

If OIG/OI and/or DOJ declines the case, the UPIC shall notify its COR and respective CPI points of contact within two (2) business days in order to move forward with the secondary administrative actions identified during the case coordination meeting.
Following this notice, the UPIC shall work with its COR, respective BFL, or suspension team member on developing the appropriate documentation for the designated secondary actions.

Regarding LE Referrals that are declined and/or returned to the I-MEDIC to take appropriate administrative action to the extent possible, should there be an outstanding overpayment that the Medicare Part C Plan Sponsor(s) could develop, upon receipt of LE's Referral declination/return, the I-MEDIC shall notify the appropriate Medicare Part C Plan Sponsor(s) of the status of the LE Referral and the outstanding overpayment, and advise the Medicare Part C Plan Sponsor(s) to move forward with the overpayment recovery efforts.

This notification shall take place within five (5) business days upon receipt of the declination/return of the LE Referral. In addition, the I-MEDIC shall document this

communication in the UCM REF record, indicating the date of the LE Referral declination/return, outstanding overpayment amount, if appropriate. The I-MEDIC shall also document the Medicare Part C Plan Sponsors impacted, the date the notification was issued to the Medicare Part C Plan Sponsors, as well as the point-of-contact at the Medicare Part C Plan Sponsor(s) who received the notification. Upon submission of this notification to the Medicare Part C Plan Sponsor(s), the I-MEDIC shall close the REF record as required.

4.18.1.2 - Immediate Advisements to the OIG/OI

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

The UPIC shall notify the OIG/OI of an immediate advisement as quickly as possible, but not more than four (4) business days after 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
- Confirmation of forged documentation during the course of an investigation, include, but is not limited to:
    - identification of forged documents through medical review; and/or
    - attestation from provider confirming forged documentation.
- Allegations and subsequent verification of services not rendered as a result of any of the following:
    - medical review findings;
    - interviews or attestations from a minimum of three (3) beneficiaries indicating that they did not receive services; and/or
    - attestations from referring/ordering providers indicating they did not refer/order a service (e.g., confirmation of no relationship with the beneficiary prior to service, or confirmed impossible day billings).
- Confirmed complaints from current or former employees that indicate the provider in question inappropriately billed Medicare for all or a majority of its services. Confirmation would be required though one of the following:
    - minimum of three (3) beneficiary interviews confirming the inappropriate billing;
    - provider attestation(s) confirming the inappropriate billing; or
    - medical review findings.
- Confirmation of beneficiary recruitment into potentially fraudulent schemes and/or provider participation (e.g., telemarketing or solicitation schemes);
- Substantiated identity theft of a provider's Medicare number, a beneficiary's Medicare number, or selling or sharing of beneficiary lists;
- Confirmed indication of patient harm (e.g., through medical review findings or confirmation of issues identified during an onsite visit or interviews with providers or beneficiaries).
- Indication of provider/supplier fraud related to national emergency, pandemic, etc.
    - Should an IA of this nature be identified, the UPIC shall notify their BFL to determine if the IA should be forwarded to a specific OIG/OI point-of-contact.

IAs should be referred to the OIG/OI only when the above criteria are met, unless prior approval is given by the COR and BFL.

Should local LE have specific parameters or thresholds in place that do not allow them to accept certain IAs, the UPIC shall notify its COR/BFL and request exemption from the applicable IA criteria in that particular jurisdiction.

When IA criteria are met, the UPICs shall perform an initial assessment to identify and document dollars currently pending payment to the provider, and/or if RAP claim payment is pending, if applicable. Should high dollar amounts be identified with either scenario, the UPIC shall notify CMS immediately, but not to exceed two (2) business days from date of identification.

Once the criteria for an IA are met, the UPIC shall notify the OIG/OI via phone or email to determine if a formal IA referral should be sent to the OIG/OI. If the IA is related to a provider/supplier that spans multiple jurisdictions, the UPIC shall notify any impacted UPIC and/or I-MEDIC Program Directors of the potential IA, allegation, and IA criteria. The UPIC shall document this communication in UCM. The UPIC shall also send notification to its COR and BFL of the potential IA. If the UPIC does not receive a response from the OIG/OI within two (2) business days (5 business days for the I-MEDIC), it shall notify its COR and BFL team and await further instructions. If the OIG/OI confirms that a formal IA should be sent, the UPIC shall provide all available documentation*, including billed/paid amounts for the YTD and the previous year,* to the OIG/OI within four (4) business days of receiving the response from OIG/OI. Upon submission of the IA to the OIG/OI, the UPIC shall request written and/or email confirmation from the OIG/OI acknowledging receipt of the IA. Simultaneously, the *UPIC* shall notify the CMS identified Strike Force points of contacts, if the notification includes providers/suppliers located within a Strike Force jurisdiction. Additionally, the UPIC shall notify and send a copy of the IA to its COR/BFL and the case coordination team, at CPIMCCNotifications@cms.hhs.gov, the same day the advisement is made to OIG/OI. In this notification to CMS, the UPIC shall advise if it has any other potential administrative actions it may want to pursue related to the provider(s)/supplier(s). The provider(s)/supplier(s) identified in an accepted IA shall be added to the UPIC's next scheduled case coordination meeting.

If the OIG/OI determines that a formal IA is not needed, the UPIC shall advise its COR/BFL and immediately continue its investigation. In instances where an IA is related to a Plan employee whistleblower, the I-MEDIC does not have to notify the case coordination team of the IA nor does the IA have to be discussed at a case coordination meeting. Rather, the I-MEDIC shall close the complaint upon acceptance and/or declination of the IA due to these complaint types being outside of the I-MEDIC's SOW.

If the IA is related to a provider/supplier that spans multiple jurisdictions, the UPIC shall send a notification to the other UPIC and/or I-MEDIC Program Directors on the same date the formal IA is sent to OIG/OI. The UPIC shall copy its COR/BFL on such communication. Upon receipt of the notification from the primary UPIC, the other UPICs and/or I-MEDIC shall provide confirmation to the primary UPIC and its COR/BFL that the notification has been received, and it is ceasing activity as instructed below. Upon receipt of acceptance or declination of the IA from the OIG/OI, the primary UPIC shall notify the other UPIC and/or I-MEDIC Program Directors of the outcome.

Upon identification and submission of an IA to the OIG/OI, unless otherwise directed, all impacted UPICs and/or I-MEDIC shall cease all investigative and administrative activities, with the exception of screening activities, data analysis, etc., until the OIG/OI responds with its acceptance or declination of the IA. If the UPIC does not receive an immediate response from the OIG/OI, the UPIC shall contact OIG/OI after two (2) business days from the date of the IA notification and document the communication in the UCM system. If the UPIC does not receive a response from the OIG/OI within five (5) business days from the date of the IA notification, the UPIC shall contact its COR/BFL for further guidance.

If the OIG/OI declines or accepts the IA, the UPIC shall document the decision in UCM and follow the processes described in Chapter 4, § 4.6.3, 4.6.4, and § 4.7 of the PIM, unless otherwise directed by CMS.

Additionally, until the necessary updates are made in the UCM, if the UPIC submits an IA based on the updated criteria, it shall select all six (6) IA options on the "External Stakeholders" page of the UCM, and notate the justification of the IA in the Record Summary section of the UCM.

During the case coordination meeting, the UPIC may receive additional guidance from CMS related to subsequent actions related to the IA. If the UPIC has questions following the case coordination meeting, the UPIC shall coordinate with its COR and BFL.

4.18.1.5 – Referral to Other Law Enforcement Agencies

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

If the OIG/OI declines a case that the UPIC believes has merit, the UPIC shall *first implement any identified secondary administrative action, and then advise their COR/BFL to determine if referral to another* law enforcement *agency*, such as the FBI*, DEA, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), RRB/OIG, and/*or MFCU, *is* appropriate. *The UPIC must receive COR/BFL approval prior to submitting a referral to another law enforcement agency, of which the UPIC shall document in the UCM.*

4.18.1.5.3 – *Reserved for Future Use*

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

4.18.2 - Referral to State Agencies or Other Organizations

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

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.

Additionally, referrals should be made to the Medicare survey and certification agency which exist in each state, 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 BFL of these referrals.

4.18.3 - UPICs and QIOs

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

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 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.

4.22 - Discounts, Rebates, and Other Reductions in Price

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

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

4.23 - Identity Theft Investigations and Victimized Provider Waiver of Liability Process

(Rev. 10711; Issued: 04-01-21; Effective: 04-19-21; Implementation: 04-19-21)

This section applies to the UPICs.

For purposes of this chapter, a "compromised number" is a beneficiary or provider/supplier number that has been stolen and used by unauthorized entities or individuals to submit claims to, i.e., bill, the Medicare program.

The UPICs shall investigate the alleged theft of provider identities. An example of provider identity theft may include a provider's identity having been stolen and used to establish a new Medicare enrollment or a new billing number (reassignment) under an existing Medicare enrollment, or updating a current Medicare provider identification number with a different electronic funds transfer (EFT) payment account causing inappropriate Medicare payments to unknown person(s) and potential Medicare overpayment and eventually, U.S. Department of Treasury (UST) debt issued to the victimized provider.

The UPICs shall discuss the identity theft case with the COR and BFL. If claims are still being submitted and Medicare payments are being made, the UPIC should pursue strategies to prevent likely overpayments from being disbursed, such as prepayment reviews, auto-denial edits, Do Not Forward (DNF) requests, or immediate payment suspensions. The purpose of these administrative actions is to stop the payments. The UPICs are not authorized to request the MAC to write-off any overpayments related to the ID theft. Prior to any enrollment actions, the UPIC should be aware of the suspected victim's reassignments and consider the effect of Medicare enrollment enforcement actions on the alleged ID theft victim's current employments.

If an actual financial harm exists as a result of the ID theft (i.e., existence of Medicare debt or overpayment determination), the UPIC will follow the Victimized Provider Project (VPP) procedures, which include the following:

- At the point in which a UPIC begins to investigate provider ID theft complaints and incurred debt, it sends a letter acknowledging receipt of the complaint, informing the

provider that CMS is investigating the complaint and reviewing materials submitted, and designating a VPP point of contact at the UPIC (IOM Pub. #100-08; Exhibit 8 – Letter 1);

- The next steps in this process include, but may not be limited to, the following:
    - Check if the case in question is in the UCM system. Vet the provider(s) with the DHHS - OIG or other appropriate LE agency to ensure that the contractor's investigative process will not interfere with prosecution;
    - A VPP case package must then be completed by the UPIC using the templates provided in the VPP information packet;
    - Describe the case and how the provider's ID was stolen or compromised. List all overpayment(s) for which the provider is being held liable. Clearly indicate those paid amounts that are in DNF and/or on payment suspension status, and the amounts that were paid with an actual check or electronic transfer to the fraudulent bank account;
    - Provide legitimate and compromised/stolen 855 forms with provider enrollment and reassignment of benefits information in order to verify legitimate PTAN(s)/NPI(s) and identify the fraudulent ones;
    - Get signed provider victim attestation statement(s) about the ID theft from the provider(s)/supplier(s).
    - Provide a police report from the alleged victim provider or any law enforcement documentation;
    - Provide financial background information, such as
        - IRS Form 1099 or W-2; and
        - Overpayment requests/debt collection notices.
    - Include any trial, DOJ and OIG documents like OIG proffers, indictment, judgments and sentencing documents; and
    - Based on the information gathered and the investigation conducted, the UPICs will state their recommendation as part of the package and provide the reason for the recommendation. Two recommendations are possible:
        - Hold provider harmless and rescind provider of federal ID theft case-related debt; OR
        - Hold provider liable for debt.

The UPIC will submit the complete VPP packet to the CMS CPI VPP team. In ID theft cases in which the victimized providers are located in multiple states and served by different UPICs, the UPIC jurisdiction in which the perpetrator's trial was located will be the lead UPIC that will coordinate with the other UPICs and submit a completed VPP packet to the CMS CPI VPP team.

The VPP team will validate and remediate all facts and information submitted by the UPIC. Part of the VPP team review may involve consultation with the HHS Office of General Counsel. This consultation may include, but may not be limited to, consideration of supporting documentation or lack thereof to support a decision that the provider is an actual victim of ID theft as well as compliance with federal statutes and regulations related to ID theft policies, debt collection and recall of overpayments.

The VPP team will make a final determination if the alleged ID theft victim is a true victim and approve a rescindment of Medicare overpayments reported in the name of the confirmed ID theft victim.

When calculating the actual overpayments related to the fraudulent claims under each provider victim, there may be situations in which discrepancies exist between LE and contractor loss calculation data. In these situations, the final figures used in making overpayment determinations should come from MAC data on amounts paid out in the name

of the victimized providers using the cleared payments transmitted to the fraudulent bank accounts established in the DOJ case.

Once a final decision is made by the VPP team, the UPIC or Lead UPIC, as appropriate, will be informed.

If the provider victim is determined to be a true victim of ID theft, the UPIC will send out a letter using the template in the IOM Pub. #100-08 Exhibits chapter informing the provider of the favorable decision and that the assessed overpayment against the victim will be rescinded ((IOM
Pub. #100-08; Exhibit 8 – Letter 2). This decision shall then flow through the UPIC to the MAC for a recall of the associated debt. (NOTE: The MAC's instructions for processing providers' debts that have been confirmed as identity theft are found in the Medicare Financial Management Manual Chapter 4, Section 110 – Confirmed Identity Theft). The MAC *shall* follow the process for making adjustments to the claims system and recall the debt registered under the victimized provider from the US Department of Treasury.

If the decision is not positive (i.e. ID theft is not confirmed), the UPIC shall correspond directly with the provider to inform him/her that CMS did not have sufficient information to confirm that identity theft has occurred. The UPIC shall send Letter 3 from the IOM Pub. #100-08 Exhibits chapter to the provider with a copy to the MAC.