CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-08 Medicare Program Integrity	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 876	**Date: April 12, 2019**
	Change Request 11109

SUBJECT: Update to Publication (Pub.) 100-08 to Provide Language-Only Changes for the New Medicare Card Project

I. SUMMARY OF CHANGES: The purpose of this Change Request (CR) is to update language-only changes for the New Medicare Card Project-related language in Pub 100-08. There are no new coverage policies, payment policies, or codes introduced in this transmittal. Specific policy changes and related business requirements have been announced previously in various communications.

EFFECTIVE DATE: May 13, 2019
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: May 13, 2019
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	2/2.3/Sources of Data for ZPICs
R	3/3.2/Overview of Prepayment and Postpayment Reviews
R	3/3.2/3.2.2.1/Maintaining Provider Information
R	3/3.6/3.6.2.5/Denial Types
R	3/3.10/Prior Authorization
R	4/Table of Contents
R	4/4.2/4.2.2.4/Procedural Requirements
R	4/4.2/4.2.2.6/Program Integrity Security Requirements
R	4/4.3/Medical Review for Program Integrity Purposes
R	4/4.6/4.6.2.1/Contact Center Operations
R	4/4.6/4.6.2.3/MAC Complaint Screening
R	4/4.6/4.6.2.4/Referrals to the UPIC
R	4/4.9/4.9.6.2/Guidelines for Incentive Reward Program Complaint Tracking
R	4/4.11/4.11.1.3/Documentation of Identity Theft and Compromised Medicare beneficiary identifiers in the FID
R	8/8.4/8.4.4.4.3/Worksheets
R	12/12.4.1/Providing Sample Information to the CERT Review Contractor
R	15/15.4/15.4.6.4/Medicare Diabetes Prevention Program (MDPP) Suppliers
R	15/15.5/15.5.19.1/Independent Diagnostic Testing Facility (IDTF) Standards
R	15/15.21/15.21.7.1/Claims against Surety Bonds
R	15/15.27/15.27.1.2.3/Reactivations – Miscellaneous Policies

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: 876	Date: April 11, 2019	Change Request: 11109

SUBJECT: Update to Publication (Pub.) 100-08 to Provide Language-Only Changes for the New Medicare Card Project

EFFECTIVE DATE: May 13, 2019
**Unless otherwise specified, the effective date is the date of service.*
IMPLEMENTATION DATE: May 13, 2019

I. GENERAL INFORMATION

A. Background: The CMS is implementing changes to remove the Social Security Number (SSN) from the Medicare card. A new number, called the Medicare Beneficiary Identifier (MBI), will be assigned to all Medicare beneficiaries. This CR contains language-only changes for updating the New Medicare Card Project language related to the MBI in Pub 100-08. The Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) requires removal of the SSN-based Health Insurance Claim Number from Medicare cards within four years of enactment. There are no new coverage policies, payment policies, or codes introduced in this transmittal. Specific policy changes and related business requirements have been announced previously in various communications.

B. Policy: MACRA of 2015.

II. BUSINESS REQUIREMENTS TABLE

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

Number	Requirement	Responsibility								
		A/B MAC			DME	Shared-System Maintainers				Other
		A	B	HHH	MAC	FISS	MCS	VMS	CWF	
11109.1	MACs shall be aware of the updated language for the New Medicare Card Project in Pub. 100-08.	X	X	X	X					

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): Tracey Mackey, 410-786-5736 or Tracey.Mackey@cms.hhs.gov , Kim Davis, 410-786-4721 or kimberly.davis@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

2.3 – Sources of Data for ZPICs

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

A. Contractors To Which This Section Applies

This section applies to ZPICs.

B. General

The ZPICs' approach for combining claims data (MAC data, Recovery Auditor data from the Recovery Auditor data warehouse) and other data to create a platform for conducting complex data analysis shall be documented in their Information Technology Systems Plan. By combining data from various sources, the ZPIC will present an entire picture of a beneficiary's claim history regardless of where the claim was processed. The primary source of this data will be the CMS shared systems data, National Claims History (NCH), and Integrated Data Repository (IDR). The ZPIC shall be responsible for obtaining data for all beneficiaries for whom the MAC(s) paid the claims.

At a minimum, ZPICs are required to store the most recent 36 months' worth of data (including Part A, Part B, DME, home health & hospice) for the jurisdiction or zone defined in their task order.

If the jurisdiction of the MAC(s) is not defined geographically, the ZPIC shall obtain a complete beneficiary claims history for each unique beneficiary for whom the MAC(s) paid a claim.

EXAMPLE 1: The MAC(s) jurisdiction covers Maryland but includes a hospital chain with facilities in Montana. The ZPIC would request claims history from shared systems, NCH, or IDR for all claims paid by the MAC(s).

EXAMPLE 2: The MAC(s) jurisdiction covers Maryland, a beneficiary lives in Pennsylvania, and the beneficiary saw a doctor in Maryland. The ZPIC would request from shared systems, NCH, or IDR for all claims paid by the MAC(s).

The ZPICs will not be able to tap data from the Common Working File (CWF).

The ZPICs should, at their discretion, if agreement and cooperation of the MAC(s) are obtained, use data directly from the claims processing system of the MAC(s), and then supplement the other data using NCH.

In developing this plan, the ZPICs shall address the above requirements and, at a minimum, establish read-only access to the MAC's shared claims processing system(s) and access to the Part A, B, and D data available through the NCH for the jurisdictional area defined in the Task Order. The ZPIC shall obtain denial data through the MACs and document the process for obtaining this data from the MAC(s) in the Joint Operating Agreement. At a minimum, the denial data shall include data for edits that were requested and/or recommended by the ZPIC.

The ZPIC shall have the ability to receive, load, and manipulate CMS data. The data shall also be maintained in accordance with CMS and Federal privacy laws and regulations as described in the CMS Data Use Agreement. For planning purposes, the ZPICs should assume that there are 30 claims per *Medicare beneficiary identifier (Mbi)* per year, on average. A claim record is about 1000 bytes. To calculate the storage space necessary, use the following formula:

(#*Mbi*s) X (30 claims) X (#years) X (1000) = #bytes

The CMS contract officer's representative (COR) and ZPIC will need to complete:

- A data use agreement to give permission to receive privacy protected data;
- A Data request form to specify all data required by the ZPIC;
- A HDC application for HDC access and/or CMS systems' access to get access to the data center and/or to specify which CMS systems the ZPIC will access;
    - A DESY system application form. (This is provided to the ZPIC post-award).

3.2 – Overview of Prepayment and Postpayment Reviews

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

This section applies to MACs, CERT, RACs, SMRCs, and ZPICs/Unified Program Integrity Contractors (UPICs), as indicated.

A. Prepayment and Postpayment Review

Prepayment review occurs when a reviewer makes a claim determination before claim payment has been made. Prepayment review always results in an "initial determination"

Postpayment review occurs when a reviewer makes a claim determination after the claim has been paid. Postpayment review results in either no change to the initial determination or a "revised determination" indicating that an overpayment or underpayment has occurred.

B. Prepayment Edit Capabilities

Prepayment edits shall be able to key on a beneficiary's *Medicare beneficiary identifier (Mbi)*, National Provider Identifier (NPI) and specialty code, service dates, and diagnosis or procedure code(s) (i.e., Healthcare Common Procedure Coding System [HCPCS] and/or International Classification of Diseases diagnoses codes), Type of Bill (TOB), revenue codes, occurrence codes, condition codes, and value codes.

The MAC systems shall be able to select claims for prepayment review using different types of comparisons. At a minimum, those comparisons shall include:

- Procedure to Procedure -permits contractor systems to screen multiple services at the claim level and in history.
- Procedure to Provider - permits selective screening of services that need review for a given provider.
- Frequency to Time- permits contractors to screen for a certain number of services provided within a given time period.
- Diagnosis to Procedure- permits contractors to screen for services submitted with a specific diagnosis. For example, the need for a vitamin B12 injection is related to pernicious anemia, absent of the stomach, or distal ileum. Contractors must be able to establish edits where specific diagnosis/procedure relationships are considered in order to qualify the claim for payment.
- Procedure to Specialty Code or TOB- permits contractors to screen services provided by a certain specialty or TOB.
- Procedure to Place of Service- permits selective screening of claims where the service was provided in a certain setting such as a comprehensive outpatient rehabilitation facility.

Additional MAC system comparisons shall include, but are not limited to the following:

- Diagnoses alone or in combination with related factors.
- Revenue linked to the health care common procedure coding system (HCPCS).

- Charges related to utilization, especially when the service or procedure has an established dollar or number limit.

- Length of stay or number of visits, especially when the service or procedure violates time or number limits.

- Specific providers alone or in combination with other parameters.

The MR edits are coded system logic that either automatically pays all or part of a claim, automatically denies all or part of a claim, or suspends all or part of a claim so that a trained clinician or claims analyst can review the claim and associated documentation (including documentation requested after the claim is submitted) in order to make determinations about coverage and payment under Section 1862(a) (1) (A) of the Act. Namely, the claim is for a service or device that is medically reasonable and necessary to diagnose or treat an injury or improve the functioning of a malformed body member. All non-automated review work resulting from MR edits shall:

- Involve activities defined under the MIP at §1893(b)(1) of the Act;

- Be articulated in the MAC's medical review strategy;

- Be designed in such a way as to reduce the MAC's CERT error rate or prevent the MAC's CERT error rate from increasing, or;

Prevent improper payments identified by the RACs.

3.2.2.1 - Maintaining Provider Information

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

This section applies to MAC.

A. Provider Tracking System (PTS)

The MACs shall have a PTS in place to identify and track all individual providers currently under action plans to correct identified problems, such, as not reasonable and necessary, incorrect coding, and inappropriate billing. MACs shall use the provider tracking system (PTS) to coordinate contacts with providers such as MR notifications, telephone calls directly related to probe reviews, and referrals to POE. The MACs shall ensure that if a provider is to be contacted as a result of more than one problem, redundant contacts are minimized. The MACs shall also coordinate corrective action information with the ZPICs to ensure contacts are not in conflict with benefit integrity related activities. The MAC PTS shall contain the date a provider is put on a provider- specific edit. The MAC shall reassess all providers on provider-specific prepayment or postpayment review on a quarterly basis to determine whether the behavior has improved. The MAC shall note the results of these quarterly assessments in the PTS. If the behavior has improved sufficiently and the edit was turned off, note that date as well in the PTS. When a MAC becomes aware that the provider has appealed a medical review determination to an Administrative Law Judge (ALJ), the MAC should send a letter to the ALJ and describe the information in the PTS to demonstrate the corrective actions that have been taken by the MAC.

B. Recovery Auditor Case Files

The Recovery Auditor shall maintain case files following the guidelines in the Recovery Auditor SOW.

C. Provider Addresses

This section applies to MACs, CERT, and Recovery Auditors, as indicated.

The MACs, CERT and Recovery Auditors shall mail the ADR to the best known address for the provider. MACs are encouraged to indicate the procedure a provider can follow to update address information in their ADRs and on their Web sites. If a provider wishes to have ADRs sent to one address but demand letters sent to a different address, MACs are encouraged to accommodate this request.

Note: Providers and suppliers must complete and submit a Medicare enrollment application (either the paper CMS-855 or a submission via Internet-based Provider Enrollment, Chain & Ownership [PECOS] to change existing information in the Medicare enrollment record.)

D. When the Provider or Supplier No Longer Occupies a Physical Address

This section applies to MACs and ZPICs, as indicated.

When the MACs and ZPICs become aware that the provider or supplier no longer occupies a physical address, any future correspondence shall reference only the claim control numbers and not list the individual beneficiary data (e.g., names and *Medicare beneficiary identifiers*). This process is contingent on current automated system limits.

The following are situations where the MAC and ZPIC can assume the provider or supplier no longer occupies the last known location. This list is not exhaustive and the MACs and ZPICs should use other means to confirm addresses, at their discretion.

- The MAC and ZPIC receive mail that has been returned by the post office indicating no known address;
- An onsite visit has confirmed the address is vacant or is occupied by another occupant; or,
- A beneficiary complaint(s) is on record stating the provider or supplier is no longer at the address and follow up confirms the complaint.

In the above situations, correspondence from the MACs and ZPICs shall only contain the claim control number and advise the provider or supplier to contact them for a list of the specific claims associated with the overpayment. This process will prevent the potential compromise of Medicare beneficiary names and/or *Medicare beneficiary identifiers* being sent to an abandoned address (or a location with a new occupant). If the letter is returned from the post office, maintain the notification on file for evidence.

3.6.2.5 - Denial Types

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

This section applies to MACs, CERT, RACs, and ZPICs/UPICs, as indicated.

A. Distinguishing Between Benefit Category, Statutory Exclusion and Reasonable and Necessary Denials

The MACs, CERT, RACs, and ZPICs/UPICs shall be cognizant that the denial type may affect the financial liability of beneficiaries. They shall ensure that benefit category denials take precedence over statutory exclusion and reasonable and necessary denials. They shall ensure that statutory exclusion denials take precedence over reasonable and necessary denials. MACs, CERT, and ZPICs/UPICs shall use the guidelines listed below in selecting the appropriate denial reason. RACs shall follow denial reason guidance outlined in their SOW.

- If additional documentation was requested from the provider or other entity for any MR reason (benefit category, statutory exclusion, reasonable/necessary, or coding), and the information is not received within 45 calendar days or a reasonable time thereafter, the MACS, CERT, and ZPICs/UPICs shall issue a reasonable and necessary denial, in full or in part.

- If additional documentation was requested because compliance with a benefit category requirement is questioned and the documentation received fails to support compliance with the benefit category, the MACs, CERT, and ZPICs/UPICs shall issue a benefit category denial.

- If additional documentation was requested because compliance with a benefit category requirement is questioned and the received documentation shows evidence that the benefit category requirement is present but is defective, the MACs, and ZPICs/UPICs shall issue a reasonable and necessary denial.

EXAMPLE 1: A MAC is conducting a review of partial hospitalization (PH) claims from a provider who has a pattern of failing to comply with the benefit category requirement that there be a signed certification in the medical record. In the first medical record, the MAC finds that there is no signed certification present in the medical record. The MAC shall deny all PH services for this beneficiary under §1835(a) (2) (F) of the Act (a benefit category denial). However, in the second medical record, the MAC determines that a signed certification is present in the medical record, but the documentation does not support the physician's certification, the services shall be denied under §1862(a) (1) (A) of the Act (a reasonable and necessary denial) because the certification is present but defective.

Example 2: The MAC performs a medical record review on a surgical procedure claim and determines that the procedure was cosmetic in nature and was not reasonable and necessary; the denial reason would be that the service is statutorily excluded since statutory exclusion denials take precedence over reasonable and necessary denials.

The MACs, CERT, RACs, and ZPICs/UPICs shall deny payment on claims either partially (e.g., by down coding or denying one line item on a multi-line claim) or in full, and provide the specific reason for the denial whenever there is evidence that a service:

- Does not meet the Benefit Category requirements described in Title XVIII of the Act, NCD, or coverage provision in an interpretive manual;

- Is statutorily excluded by other than §1862(a)(1) of the Act;

- Is not reasonable and necessary as defined under §1862(a) (1) of the Act. MACs, CERT, RACs, and ZPICs/UPICs shall use this denial reason for all non-responses to documentation requests;

- Was not billed in compliance with the national and local coding, payment or billing requirements; and/or

- Was not delivered or provided to the beneficiary, or not provided as billed.

The denial explanation needs to be more specific than merely repeating one of the above bullets. The general exception to the need for a full denial explanation is in the event of a clerical error, for example, the billing entity transposes two digits in the *Medicare beneficiary identifier* on a claim. The claim is quickly

returned, usually electronically, to the provider for correction. In the case of dual-eligible beneficiaries where there is a State-specific policy, see CMS IOM Pub. 100-04, chapter 30, §60.5 A for a detailed explanation of handling administrative denials.

3.10 – Prior Authorization

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

A. Overview

Prior authorization is a process through which a request for provisional affirmation of coverage is submitted to CMS or its contractors for review before the item or service is furnished to the beneficiary and before the claim is submitted for processing. It is a process that permits the submitter (e.g., provider, supplier, beneficiary, etc.) to send in medical documentation in advance of providing and billing for an item or service, to verify its eligibility for Medicare claim payment. Contractors shall, at the direction of CMS or other authorizing entity, conduct prior authorizations and alert the submitter of any potential issues with the information, as submitted.

For any item or service to be covered by Medicare it must:

- Be eligible for a defined Medicare benefit category,
- Be medically reasonable and necessary for the diagnosis or treatment of illness or injury or to improve the functioning of a malformed body member, and
- Meet all other applicable Medicare coverage, coding and payment requirements.

Contractors shall communicate to the submitter (and beneficiary upon request) their prior authorization decision and the assigned unique tracking number (UTN), which indicates that the submitter requested a prior authorization, for corresponding claim submissions.

For certain prior authorization programs, the requirement to prior authorize is a condition of payment, as further described in the sections below.

Absent any explicit CMS instruction to the contrary, submitters may correct identified issues with their prior authorization request(s) and resubmit their request(s) for prior authorization without restriction. Contractors shall conduct prior authorization reviews within the timeframes defined by CMS in the corresponding prior authorization program operational instruction(s).

The prior authorization process is further described in following sections.

B. Condition of Payment

Contractors shall determine if the requirement to prior authorize a particular item or service is a condition of payment, as specified in the individual operational instruction(s). If prior authorization is a condition of payment, claims submitted without an indication that the submitter made a prior authorization request (i.e., UTN) shall be denied upon receipt.

C. Outreach and Education

Contractors shall educate stakeholders each time a new prior authorization program is launched for a particular item or service, the requisite information and timeframes for prior authorization submissions, and the vehicle(s) for submitting such information to the contractor for assessment. Contractors shall make sure submitters are aware of the timeframes for contractors to render prior authorization decisions, for each individual prior authorization program.

Each prior authorization program will have an associated Operational Guide and will be available on the CMS website. Contractors shall, at a minimum, provide public access to agency-developed prior authorization operational guides, by posting the link(s) on their website.

Contractors shall hold group or individualized training sessions, as appropriate, to notify the stakeholders of upcoming prior authorization programs and to make sure there is ongoing understanding of the specific requirements for those applicable prior authorization programs.

D. Prior Authorization Submission

Contractors shall assess the information/documentation included in the prior authorization submission for completeness. Requisite information for individualized prior authorization programs will be included in the operational guides, and shall be available on the CMS website.

Requisite information may include, but is not limited to:

- Beneficiary Information (i.e., name, *Medicare beneficiary identifier*, date of birth)
- Physician/Practitioner Information (i.e., name, provider identification number, address)
- Supplier Information (i.e., name, national supplier clearinghouse (NSC) number, identification number, address)
- Documentation from the medical record to support the medical necessity of the item or service, and
- Any other relevant documents as deemed necessary by the contractor to process the prior authorization.

E. Prior Authorization Decisions

Contractors shall notify the submitter if their prior authorization submission results in a provisional affirmative, or non-affirmative decision.

- A provisional affirmative decision is a preliminary finding that a future claim submitted to Medicare for the item or service likely meets Medicare's coverage, coding, and payment requirements.
- A non-affirmative decision is a finding that the submitted information/documentation does not meet Medicare's coverage, coding, and payment requirements, and if a claim associated with the prior authorization is submitted for payment, it would not be paid. Contractors shall provide notification of the reason(s) for the non-affirmation, if a request is non-affirmative, to the submitter. If a prior authorization request receives a non-affirmative decision, the prior authorization request can be resubmitted an unlimited number of times, unless otherwise specified.

Contractors shall send detailed decision letters to submitters. As appropriate for the given prior authorization program, contractors shall send detailed decision letters to other stakeholders (e.g., beneficiaries) using their official address on file. In addition, there may be certain prior authorization programs that require the contractors to notify the appropriate entity by other means, such as telephone.

If a claim is submitted for payment without an affirmative prior authorization decision on file, contractors shall use their existing processes to either suspend claims for additional review or to process claims as denials, based on each individualized prior authorization program, as detailed in the operational instruction.

F. Expedited Request

For certain items or services, delays in receipt of a prior authorization decision could jeopardize the life or health of the beneficiary. Contractors shall, for such items or services, expedite their decisions based on the operational instruction.

If the claim processing systems would unavoidably delay the delivery of the UTN in an expedited fashion, contractors shall nonetheless render an affirmative or non-affirmative decision to the submitter within the mandated, expedited timeframe. Contractors shall alert the submitter that the decision is being provided as expediently as possible, so that the item or service may be provided, but that the submitter should hold their claim and not submit it until such time as the UTN is received (in order to avoid a claims payment denial).

Medicare Program Integrity Manual
Chapter 4 - Program Integrity

Table of Contents
(Rev.876; Issued: 04-12-19)

Transmittals for Chapter 4

4.2.2.4 - Procedural Requirements

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

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, *Medicare beneficiary identifier (Mbi)*, nature of the referral, date the referral is forwarded to the UPIC, name and contact information of the individual who made the referral, and the name of the UPIC to whom the referral was made.

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

- Refer potential fraud, waste, or abuse situations promptly to the UPIC;
- Forward complaints alleging fraud through the screening staff to the UPIC;
- Maintain confidentiality of referrals to the UPIC;
- Forward to the UPIC detailed documentation of telephone or personal contacts involving fraud issues discussed with providers/suppliers or provider/supplier staff, and retain such information in individual provider/supplier files; and
- The UPIC shall ensure the performance of the functions below and have written procedures for implementing these functions:

Investigations

- Keep educational/warning correspondence with providers/suppliers and other fraud documentation concerning specific issues in individual provider/supplier files so that 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).

- 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 FID, provide ideas and feedback on Fraud Alerts and/or vulnerabilities within the Medicare or Medicaid programs.

• Report to the COR and IAG BFL all situations that have been identified where a provider consistently fails to comply with the provisions of the assignment agreement.

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

Law Enforcement

• Serve as a reference point for LE and other organizations and agencies to contact when they need help or information on Medicare fraud issues and do not know whom to contact.

• Hire and retain employees who are qualified to testify in a criminal and civil trial when requested by LE.

• Provide support to LE agencies for investigation of potential fraud, including those for which an initial referral to LE did not originate from the UPIC.

• Meet (in person or via telephone call) with the OIG agents to discuss pending or potential cases, as necessary.

• Meet (in person or via telephone) when needed with the DOJ to enhance coordination on current or pending cases.

• Furnish all available information upon request to the OIG/OI with respect to excluded providers/suppliers requesting reinstatement.

• Notify via e-mail the COR and IAG BFL who will obtain approval or disapproval when the UPIC is asked to accompany the OIG/OI or any other LE agency onsite to a provider/supplier for the purpose of gathering evidence in a potential fraud case (e.g., executing a search warrant). However, LE must make clear the role of UPIC personnel in the proposed onsite visit. The potential harm to the case and the safety of UPIC personnel shall be thoroughly evaluated. The UPIC personnel shall properly identify themselves as UPIC employees and under no circumstances shall they represent themselves as LE personnel or special agents. Lastly, under no circumstances shall UPIC personnel accompany LE in situations where their personal safety is in question.

• Maintain independence from LE and do not collect evidence, i.e., request medical records or conduct interviews, at their request. The UPIC is expected to follow the current vetting process and the requirements of PIM Sections 4.41 G, K and L. The UPIC shall consult with the BFLs and CORs if questions arise about complying with LE requests for medical records, conducting interviews, or refraining from specific administrative actions.

Training

- Work with the COR and IAG BFL to develop and organize external programs and perform training, as appropriate, for LE, ombudsmen, grantees (e.g., Senior Medicare Patrols), and other CMS health care partners (e.g., Administration on Aging (AoA), state MFCUs).

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

- Assist in preparing and developing fraud-related articles for MAC newsletters/bulletins. Once completed, the UPIC shall submit such materials to the following email address: CPIFraudRelatedLeads@cms.hhs.gov, with a copy to the CORs and IAG BFLs.

- Provide resources and training for the development of existing employees and new hires.

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

- Ensure no payments are made for items or services ordered, referred, or furnished by an individual or entity following the effective date of exclusion (refer to § 4.19, for exceptions).

- Ensure all instances where an excluded individual or entity that submits claims for which payment may not be made after the effective date of the exclusion are reported to the OIG (refer to PIM, chapter 8,).

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

4.2.2.6 – Program Integrity Security Requirements

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

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, *Medicare beneficiary identifiers*, 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 *Medicare beneficiary identifiers* 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 IAG BFLs for approval prior to release. This includes, but is not limited to, contractor initiated press releases, media questions, media interviews, and Internet postings.

F. Computer Security

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

G. Telephone and Fax Security

The 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.

4.3 – Medical Review for Program Integrity Purposes

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

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

- Possible falsification or other evidence of alterations of medical record documentation including, but not limited to: obliterated sections; missing pages, inserted pages, white out; and excessive late entries;

- Evidence that the service billed for was actually provided and/or provided as billed; or,
- Patterns and trends that may indicate potential fraud, waste, and abuse.

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

- Section 1833(e), which states in part "...no payment shall be made to any provider... unless there has been furnished such information as may be necessary in order to determine the amounts due such provider ...;"

- Section 1842(a)(2)(B), which requires MACs to "assist in the application of safeguards against unnecessary utilization of services furnished by providers ...; "

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

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

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

- Sections 1812, 1861, and 1832, which describe the Medicare benefit categories; and

- Sections 1874, 1816, and 1842, which provide further authority.

The regulatory authority for the MR program rests in:

- 42 CFR §421.100 for intermediaries.

- 42 CFR §421.200 for carriers.

- 42 CFR §421.400 for MACs.

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

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

It is essential that MR is integrated early in the investigative plan of action to facilitate the timeliness of the investigative process. Before deploying significant MR resources to examine claims identified as potentially fraudulent, the UPIC may perform a limited prepayment MR to help identify signs of potential fraud, waste,

or abuse. The general recommendation for a provider/supplier specific edit would be to limit the prepayment MR to specific procedure codes, a specific number of claims, or based on a particular subset of beneficiaries identified through the UPIC's analysis. Another option may be for the UPIC to perform a MR probe to validate the data analysis or allegation by selecting a small representative sample of claims. The general recommendation for a provider/supplier-specific probe sample is 20-40 claims. This sample size should be sufficient to determine the need for additional prepayment or post-payment MR actions. MR resources shall be used efficiently and not cause a delay in the investigative process. In addition, development of an investigation shall continue while the contractor is awaiting the results of the MR.

A. Referrals from the Medicare Administrative Contractor or Recovery Audit Contractor to the Unified Program Integrity Contractor

If a provider/supplier appears to have knowingly and intentionally furnished services that are not covered, or filed claims for services not furnished as billed, or made any false statement on the claim or supporting documentation to receive payment, the MAC or RAC personnel may discuss potential referral of the matter to the UPIC. If the UPIC agrees that there is potential fraud, waste, and/or abuse, the MAC or RAC personnel shall escalate and refer the matter to the UPIC.

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

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

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

The UPICs are also responsible for preventing and minimizing the opportunity for fraud. The UPICs shall identify procedures that may make Medicare vulnerable to questionable billing or improper practices and take appropriate action.

CMS has implemented recurring edit modules in all claims processing systems to allow UPICs and/or CMS to monitor specific beneficiary and/or provider/supplier numbers and other claims criteria. When appropriate, the UPIC may request the MAC to install a prepayment or auto-denial edit. The MACs shall comply with requests from UPICs and/or CMS to implement those edits. The MACs shall implement parameters for those edits/audits within the timeframe established in the MAC and UPIC JOA, which shall not exceed more than 15 business days.

C. Program Integrity/Medical Review Determinations

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

1. The UPIC shall maintain current references to support MR determinations. The review staff shall be familiar with the below references and be able to track requirements in the internal review guidelines back to the statute or manual. References include, but are not limited to:

- CFRs;

- CMS Internet Only Manuals (IOMs);

- Local coverage determinations (LCDs);

- National coverage determinations (NCDs); and

- Internal review guidelines (sometimes defined as desktop procedures).

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

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

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

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

- The medical records tend to have obvious or nearly identical documentation.

- In reviews that cover a sequence of codes (e.g., evaluation and management codes, therapies, radiology), evidence may exist of a trend to use with greater frequency than would be expected the high-end billing codes representing higher level services.

- In a provider/supplier review, a pattern may be identified of billing more hours of care than would normally be expected on a given workday.

- The medical records indicate a procedure is being done more frequently than prescribed per suggested CMS guidance or industry standards of care, resulting in potential situations of patient harm.

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

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

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

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

D. Quality Assurance

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

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

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

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

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

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

Automated edits shall be evaluated annually.

Prepayment edits shall be evaluated on a quarterly basis. They shall be analyzed in conjunction with data analysis to confirm or re-establish priorities. For example, a prepayment edit is implemented to stop all claims with a specific diagnostic/procedure code and the provider stops submitting claims with that code to circumvent the edit.

Data analysis shall be used to identify if the provider's general billing pattern has changed in volume and/or to another/similar code that may need to be considered/evaluated to revise the current edit in question and/or expansion of the current investigation.

4.6.2.1 – Contact Center Operations

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new

Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.
The Contact Center Operations (CCO) is a CMS managed contact center which provides beneficiaries with personalized Medicare information and accepts both inquiries and complaints regarding a variety of topics including, but not limited to, billing errors, the provision of services/tests, and coverage guidelines.

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

- Lab Tests - CSRs shall ask callers if they recognize the referring physician. If they do, remind callers that the referring physician may have ordered some lab work for them. The beneficiaries usually do not have contact with the lab because specimens are sent to the lab by the referring physician office. (Tip: ask if they remember the doctor withdrawing blood or obtaining a tissue sample on their last visit).

- Anesthesia Services - CSRs shall check the beneficiary claims history for existing surgery or assistant surgeon services on the same date. If a surgery charge is on file, explain to the caller that anesthesia service is part of the surgery rendered on that day.

- Injections - CSRs shall check the beneficiary claim history for the injectable (name of medication) and the administration. Most of the time, the administration of the injection is not payable, as it is a bundled service under Part B only. There are very few exceptions to pay for the administration.

- Services for Spouse - If the beneficiary states that services were rendered to their spouse, the CSR shall initiate the overpayment processes. *The CSR should advise the beneficiary to have the provider file a claim with the correct Medicare beneficiary identifier.*

- Billing Errors - If the beneficiaries state that they already contacted their provider/supplier and the provider/supplier admitted there was a billing error but a check is still outstanding, the CSR shall follow the normal procedures for resolving this type of billing error.

- Services Performed on a Different Date - The beneficiaries state that a service was rendered, but on a different date. The CSR shall review the beneficiary claim history to determine if there are multiple dates billed for this service. If not, an adjustment to the claim may be required to record the proper date on the beneficiaries' file.

- Incident to Services - Services may be performed by a nurse in a doctor's office as "incident to." These services are usually billed under the physician's provider/supplier transaction access number (PTAN) (e.g., blood pressure check, injections). These services may be billed under the minimal evaluation and management codes.

- Billing Address vs. Practice Location Address - The CSR shall check the practice location address where services were rendered. Many times the Medicare
Summary Notice will show the billing address, causing the beneficiaries to think the billing might be fraud.

The CSRs shall use proper probing questions and shall use claim history files to determine if the complaint or inquiry needs to be referred to the MAC for additional screening.

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

Immediate advisements (IA) shall be referred immediately to the MAC for handling and screening. These advisements include inquiries or allegations by beneficiaries or providers/suppliers concerning kickbacks, bribes, or a crime by a federal employee (e.g., altering claims data or manipulating them to create preferential treatment to certain providers/suppliers; improper preferential treatment collecting overpayments; or embezzlement). Indicators of contractor employee fraud shall be forwarded to the CMS Compliance Group.

4.6.2.3 – MAC Complaint Screening

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

A. MAC Screening of CCO Referrals

The MAC shall only screen potential fraud, waste, and abuse complaints, inquiries referred by the CCO with a paid amount of $100 or greater (including the deductible as payment), or three (3) or more beneficiary complaints or inquiries, regardless of dollar amount, about the same provider/supplier. Complaints or inquiries that do not meet the above threshold for screening shall be closed. Each complaint or inquiry shall be tracked and retained for one (1) year. Beneficiaries inquiring about complaints should be advised that they are being tracked and reviewed. The MAC shall perform a more in-depth review if additional complaints or inquiries are received. The MAC shall enter all potential fraud, waste, and abuse complaints or inquiries received from beneficiaries into their internal tracking system. The MAC shall maintain a log of all potential fraud, waste, and abuse complaints or inquiries received from the CCO. At a minimum, the log shall include the following information:

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

The MAC staff may call the beneficiary or the provider/supplier, check claims history, and check provider/supplier correspondence files for educational or warning letters or contact reports that relate to similar complaints or inquiries, to help determine whether or not there is a pattern of potential fraud, waste, and abuse. The MAC shall request and review certain documents, such as itemized billing statements and other pertinent information, as appropriate, from the provider/supplier. If the MAC is unable to make a

determination on the nature of the complaint or inquiry (e.g., fraud, waste, and abuse, billing errors) based on the aforementioned contacts and documents, the MAC shall order medical records and limit the number of medical records ordered to only those required to make a determination. The MAC shall only perform a billing and document review on medical records to verify that services were rendered. If fraud, waste, and abuse are suspected after performing the billing and document review, the medical records shall be forwarded to the UPIC for review in accordance with the referral timeframe identified below.

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

B. Screening of OIG Hotline Referrals

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

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

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

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

If the MAC determines that the complaint or inquiry is not a fraud and/or abuse issue, and if the MAC discovers that the complaint or inquiry has other issues (e.g., MR, enrollment, claims processing), it shall be referred to the appropriate department and then closed.

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

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

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

The MAC shall identify and refer complaints alleging fraud, waste, or abuse in the Medicare Part C or Part D programs to the MEDIC. This includes complaints that do not have a credible allegation of fraud. The MAC shall identify and refer complaints alleging fraud, waste, or abuse involving the Federal Marketplace and State-Based Exchanges, insurance agents/brokers marketing Marketplace plans, and Marketplace consumers to the following email address: marketplaceintegrity@cms.hhs.gov, with a copy to the MAC CORs. The MAC shall close the complaint in its internal tracking system. These referrals shall be done in accordance with the timeframes established above.

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

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

4.6.2.4 - Referrals to the UPIC

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

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

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

- Claims may have been altered

- Claims have been up-coded to obtain a higher reimbursement amount and appear to be fraudulent or abusive;

- Documentation appears to indicate that the provider/supplier has attempted to obtain duplicate reimbursement (e.g., billing both Medicare and the beneficiary for the same service or billing both Medicare and another insurer in an attempt to be paid twice). An example of an attempt to obtain duplicate reimbursement might be that a provider/supplier has submitted a claim to Medicare, and then in two (2) business days resubmits the same claim in an attempt to bypass the duplicate edits and gain double payment. This apparent double-billing does not include routine assignment violations. The MAC shall attempt to resolve all routine assignment violations. However, referral from the MAC to the UPIC shall be made in instances where the provider/supplier has repeatedly committed assignment violations, indicating a potential pattern;

- Potential misrepresentation with respect to the nature of the services rendered, charges for the services rendered, identity of the person receiving the services, identity of persons or doctor providing the services, dates of the services, etc.;

- Alleged submissions of claims for non-covered services are misrepresented as covered services, excluding demand bills and those with Advanced Beneficiary Notices (ABNs);

- Claims involving potential collusion between a provider/supplier and a beneficiary resulting in higher costs or charges to the Medicare program;

- Alleged use of another person's *Medicare beneficiary identifier* to obtain medical care;

- Alleged alteration of claim history records to generate inappropriate payments;

- Alleged use of the adjustment payment process to generate inappropriate payments; or

- Any other instance that is likely to indicate a potential fraud, waste, and abuse situation.

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

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

- Provider/supplier name, NPI, provider/supplier number, and address.

- Type of provider/supplier involved in the allegation and the perpetrator, if an employee of the provider/supplier.

- Type of service involved in the allegation.

- Place of service.

- Nature of the allegation(s).

- Timeframe of the allegation(s).

- Narration of the steps taken and results found during the MAC's screening process (discussion of beneficiary contact, if applicable, information determined from reviewing internal data, etc.).

- Date of service, procedure code(s).

- Beneficiary name, beneficiary *Medicare beneficiary identifier*, telephone number.

- Name and telephone number of the MAC employee who received the complaint.

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

The MAC shall maintain a copy of all referral packages.

4.9.6.2 - Guidelines for Incentive Reward Program Complaint Tracking

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new

Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

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

- Name;
- *Medicare beneficiary identifier* or Social Security number (for non-beneficiary complaints);
- Address;
- Telephone number; or

Any other requested identifying information needed to contact the individual.
The UPIC shall refer cases to the OIG for investigation if referral criteria are met according to PIM Chapter 4, §4.18.1 - Referral of Cases to the Office of the Inspector General (OIG). The case report shall also be forwarded to the OIG.
The UPIC shall enter all available information into the IRP tracking database. Information that shall be maintained on the IRP tracking database includes:

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

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

4.11.1.3 - Documentation of Identity Theft and Compromised *Medicare beneficiary identifiers* in the FID

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

This section applies to ZPICs.

When entering identity theft investigations into the FID, the ZPIC shall enter the information for the "Compromised" provider/supplier number as the primary subject (i.e., the false or "compromised" number; the provider/supplier who stole the identity; the "false front" provider/supplier; the new provider/supplier location for which the real provider/supplier did not submit a Form CMS-855 change request; and/or the group practice to which a physician attests he/she did not reassign his/her benefits). This information shall include both the NPI and PTAN associated with that provider/supplier as well as the street address and as much detail as possible (e.g., ownership, employer identification number (EIN), electronic funds transfer (EFT), bank account, revocation/deactivation information, billing company, registered agent). The ZPIC shall clearly indicate the information associated with the "Compromised" provider/supplier number, the primary subject. The ZPIC shall differentiate this from the number and information associated with the "Legitimate" provider/supplier number.

The ZPIC shall enter information on the provider's/supplier's "Legitimate" provider/supplier number (i.e., the "real" number of the provider/supplier whose identity was stolen or compromised) only in the narrative, including the NPI and PTAN associated with the provider/supplier along with the street address and all of the background information (ownership, EIN, EFT, bank account, revocation/deactivation information,

billing company, registered agent, etc.), clearly displaying it as associated with the “Legitimate” provider/supplier number.

8.4.4.4.3 - Worksheets

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

The PSC or ZPIC BI units or the contractor MR units shall maintain documentation of the review and sampling process. All worksheets used by reviewers shall contain sufficient information that allows for identification of the claim or item reviewed. Such information may include, for example:

- Name and identification number of the provider or supplier;
- Name and title of reviewer;
- The *Medicare beneficiary identifier (Mbi)*, the unique claim identifier (e.g., the claim control number), and the line item identifier;
- Identification of each sampling unit and its components (e.g., UB-92 or attached medical information)
- Stratum and cluster identifiers, if applicable;
- The amount of the original submitted charges (in column format);
- Any other information required by the cost report worksheets in PIM Exhibits 9 through 12;
- The amount paid;
- The amount that should have been paid (either over or underpaid amount); and,
- The date(s) of service.

12.4.1 - Providing Sample Information to the CERT Review Contractor

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19 Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

All data exchanged between the CMS Data Center (CMSDC) and the MAC virtual datacenters shall be in an electronic format via NDM CONNECT:DIRECT.

The MAC virtual data centers shall submit a daily file containing information on claims entered during the day, in the formats specified in instructions available to a MAC CERT Point of Contact. MAC virtual data center responses to requests from the CERT program for claim information, shall follow the same instructions.

A. Claims Universe File

The shared systems will create a mechanism for the MAC virtual data centers to be able to create the claims universe file, which will be transmitted daily to the CMSDC. The file will be processed through a sampling module residing on the server at CMSDC. The data centers shall ensure that the claims universe file contains all claims except home health agency request for anticipated payment claims that have entered the shared claims processing system.

Canceled claims are included in the claims universe file because the decision to cancel the claim has not been made by the time the claims universe file is submitted. The data centers shall ensure that each claim included in the universe file is unique and may only be selected on the day it enters the system.

B. Sampled Claims Transaction File

The shared systems shall create a mechanism for the data centers to receive a sampled claims transaction file from the CMS DC on a daily basis. This file will include claims that were sampled from the daily claims universe files.

C. Sampled Claims Resolution File and Claims History Replica File

The shared systems shall create a mechanism for the data centers to match the sampled claims transaction file against the shared system claims history file to create a sampled claims resolution file and a claims history replica file. The claims history replica file is comprised of the claims history data file in the shared system format. These files shall be transmitted at the same time to the CMSDC. The resolution file is input to the CERT claim resolution process and the claims history replica file is added to the Claims History Replica database.

The MAC data center shall furnish resolution information for all finalized claims included in the transaction file within five days of receipt of a request from the CERT review contractor. MACs receiving daily transaction files shall respond with resolution files (on a daily basis for Part A and DME, weekly for Part B). Resolution information on claims that have not finalized by the initial request shall be included at the first opportunity immediately after the claim has finalized.

The MAC data center shall provide the sampled claims resolution file(s) and the claims history replica file(s) for each iteration of the claim when the claim number changes within the shared system as a result of adjustments, replicates, or other actions taken by the MAC. The sampled claims transaction file will always contain the claim control number of the original claim.

D. Claims with Multiple Versions

In many cases, after a provider submits a claim, a contractor or shared system or provider will submit an "adjustment claim," "split claim," or a "replicate claim." An initial claim can have multiple adjustments or iterations made to it. When the sampled claim has been adjusted or otherwise has multiple versions linked to the sampled claim in the MAC claim processing system, the resolution file contains a separate record for each version of the claim. The CERT review contractor shall review the most current version of the claim that finalized before the date of the transaction file. The CERT review contractor shall not review any version of the claim that finalized after the date of the transaction file. The CERT review contractor shall use the claim adjudication date in the resolution record to determine when the claim finalized.

E. No Resolution Claims

If a claim identified on the transaction file is not found on the shared system claims history file, no record should be created for that claim. These are called no-resolution claims. Each MAC shall take all necessary steps to minimize the number of no- resolution claims it submits to the CERT review contractor each year. The MAC may obtain a list of no-resolution claims for a given time period on either the Status Summary of Sample Claims page or the All Sampled Claims page of the Claims Status website (CSW). If the MAC receives a request for a claim for which the shared system is not able to produce a resolution file, the MAC shall research the claim to determine why a resolution record was not produced.

When the MAC identifies a no-resolution claim where the *Mbi* on the finalized claim is different from the *Mbi* on the transaction request, the MAC shall notify the CERT review contractor of the correct *Mbi*. The MAC shall not enter an acceptable no- resolution reason code for claims that finalized with a *Mbi that is* different from *that* on the transaction request.

No-resolution claims with acceptable no-resolution reasons, which are entered by the CERT Point of Contact, will not be in the no-resolution rate. Should the MAC discover that one or more no-resolution claims has an acceptable reason, the MAC shall enter the appropriate acceptable no- resolution reason code on the CSW.

The MAC shall keep documentation on file that supports the acceptable no-resolution reason. The MAC shall make this documentation available to CMS or the Office of Inspector General upon request.

F. Provider Address File

In addition to the claim resolution file, each MAC data center shall transmit the provider address file containing the names; known addresses; and telephone numbers of all the billing, attending, ordering/referring, and performing/rendering providers for all the claims on the resolution file. Each unique provider and address combination shall be included only once on each provider address file.

15.4.6.4 – Medicare Diabetes Prevention Program (MDPP) Suppliers

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

A. General Background Information

The Diabetes Prevention Program (DPP) is a structured lifestyle intervention that includes dietary coaching, lifestyle intervention, and moderate physical activity, all with the goal of preventing the onset of diabetes in individuals who are pre-diabetic. The clinical intervention consists of 16 intensive "core" sessions of a curriculum in a group-based, classroom-style setting that provides practical training in long-term dietary change, increased physical activity, and behavior change strategies for weight control. After the 16 core sessions, less intensive monthly follow-up sessions help ensure that the participants maintain healthy behaviors. The primary goal of the intervention is lowering the progression to type 2 diabetes, measured using a proxy of at least 5 percent average weight loss among participants.

The Center for Medicare & Medicaid Innovation (CMMI) first tested the DPP program in the Medicare population through a Round One Health Care Innovation Award (HCIA). In March 2016, Department of Health and Human Services (HHS) announced that the Centers for Medicare & Medicaid Services (CMS) Office of the Actuary (OACT) certified the pilot DPP model as a cost savings program that reduced net Medicare spending. The Secretary then determined that the program demonstrated the ability to improve the quality of patient care without limiting coverage or benefits. Together, these determinations fulfilled CMMI's model expansion requirements of Section 1115A of the Social Security Act.

As a result, CMMI expanded the initial HCIA model test into a national Medicare DPP (MDPP) model where organizations furnish MDPP services to beneficiaries with an indication of pre-diabetes for one year, and individuals who meet certain performance goals may continue eligibility to receive MDPP services through monthly ongoing maintenance sessions for up to an additional year.

B. MDPP Suppliers Eligibility and Enrollment Requirements

An entity or individual who wishes to furnish MDPP services –to Medicare beneficiaries must enroll as an "MDPP supplier" via the Form CMS-20134. Such suppliers must meet the following requirements:

- Have MDPP preliminary recognition, as defined at 42 CFR 424.205 or full recognition as determined by the Center for Disease Control and Prevention's (CDC) Diabetes Prevention Recognition Program (DPRP)

- Obtained and maintained valid TIN and NPI at the organizational level

- Passed application screening at a high categorical risk level per § 424.518(c) upon initial enrollment and revalidate at moderate categorical risk level per § 424.518(b), and

- Complies with the supplier standards.

As noted above, MDPP supplier applicants do not require any licensure, accreditation, or certificates to be eligible to enroll as an MDPP supplier. Rather, the CDC administers the curriculum for the DPP and monitors organization's fidelity to and success with furnishing the services. Thus, organizations with preliminary or full recognition from the CDC's DPRP indicate that they are prepared to deliver MDPP services.

As a part of the expanded CMMI model, CMS will only accept in-person MDPP suppliers to enroll into Medicare. Though an entity may furnish a select number of virtual MDPP make up sessions to a beneficiary (no more than 4 per beneficiary over the entire period of MDPP services), they would still be considered in-person MDPP suppliers.

C. MDPP Supplier Standards

All MDPP suppliers must comply with MDPP supplier standards in order to obtain and retain Medicare billing privileges. Consistent with 42 CFR §424.205(d), each MDPP Supplier must certify on its Form CMS-20134 enrollment application that it meets and will continue to meet the following standards and all other requirements:

- must have and maintain MDPP preliminary recognition, or full CDC DPRP recognition.
- must not currently have its billing privileges terminated or be excluded by a state Medicaid agency.
- must not permit MDPP services to be furnished by or include on its roster any individual coach who meets ineligibility criteria.
- must maintain at least one administrative location on an appropriate site. All administrative locations, must be reported on their CMS-20134 form and may be subject to site visits.
- must update this enrollment application within 30 days for any changes of ownership, changes to the coach roster, and final adverse legal action history and update all other changes within 90 days.
- must maintain a primary business telephone that is operating at administrative locations or directly where services are furnished. The associated telephone number must be listed with the name of the business in public view.
- must not convey or reassign a supplier billing number.
- must not deny an MDPP beneficiary access to MDPP services during the MDPP benefit period, including conditioning access to MDPP services on the basis of an MDPP beneficiary's weight, health status, or achievement of performance goals, with certain exemptions.
- must offer MDPP beneficiaries the entirety of the MDPP benefit to which they are eligible.
- must not, nor may other individuals or entities performing functions or services related to MDPP on the MDPP supplier's behalf, directly or indirectly commit any act or omission, or adopt any policy that coerces or otherwise influences an MDPP beneficiary's decision to begin accessing MDPP services, or change to a different MDPP supplier specifically.
- must disclose detailed information about the MDPP benefit to each beneficiary to whom it furnishes MDPP services before the initial core session is furnished, including the set of services, eligibility requirements, the once per lifetime nature of the MDPP benefit, and these standards.
- must answer MDPP beneficiaries' questions about MDPP services and respond to MDPP related complaints. An MDPP supplier must implement a complaint resolution protocol and maintain documentation of all beneficiary contact regarding such complaints, including the name and *Medicare beneficiary identifier* of the beneficiary, a summary of the complaint, related correspondences, notes of actions taken, and the names and/or NPIs of individuals who took such action on behalf of the MDPP supplier. This information must be kept at each administrative location and made available to CMS or its contractors upon request.
- must maintain a crosswalk file which indicates how participant identifications for the purposes of CDC performance data correspond to corresponding beneficiary health insurance claims numbers or *Medicare beneficiary identifiers* for each MDPP beneficiary. The MDPP supplier must submit the crosswalk file to CMS or its contractor.
- must submit performance data for MDPP beneficiaries who attend ongoing maintenance sessions with data elements consistent with the CDC's DPRP Standards for data elements required for the core benefit.
- must allow CMS or its agents to conduct onsite inspections or recordkeeping reviews in order to ascertain the MDPP supplier's compliance with these standards, as well as documentation requirements.

Violations of such standards are determined as non-compliance, and the associated enrolment denial and

revocation authorities would apply.

15.5.19.1 – Independent Diagnostic Testing Facility (IDTF) Standards

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

A. IDTF Standards

Consistent with 42 CFR §410.33(g), each IDTF must certify on its Form CMS-855B enrollment application that it meets the following standards and all other requirements:

1. Operates its business in compliance with all applicable Federal and State licensure and regulatory requirements for the health and safety of patients.

    - The purpose of this standard is to ensure that suppliers are licensed in the business and specialties being provided to Medicare beneficiaries. Licenses are required by State and/or Federal agencies to make certain that guidelines and regulations are being followed and to ensure that businesses are furnishing quality services to Medicare beneficiaries.

    - The responsibility for determining what licenses are required to operate a supplier's business is the sole responsibility of the supplier. The contractor is not responsible for notifying any supplier of what licenses are required or that any changes have occurred in the licensure requirements. No exemptions to applicable State licensing requirements are permitted, except when granted by the State.

    - The contractor shall not grant billing privileges to any business not appropriately licensed as required by the appropriate State or Federal agency. If a supplier is found providing services for which it is not properly licensed, billing privileges may be revoked and appropriate recoupment actions taken.

2. Provides complete and accurate information on its enrollment application. Changes in ownership, changes of location, changes in general supervision, and final adverse actions must be reported to the contractor within 30 calendar days of the change. All other changes to the enrollment application must be reported within 90 days.

    NOTE: This 30-day requirement takes precedence over the certification in section 15 of the Form CMS-855B whereby the supplier agrees to notify Medicare of any changes to its enrollment data within 90 days of the effective date of the change. By signing the certification statement, the IDTF agrees to abide by all Medicare rules for its supplier type, including the 30-day rule in 42 CFR §410.33(g)(2).

3. Maintain a physical facility on an appropriate site. (For purposes of this standard, a post office box, commercial mailbox, hotel, or motel is not an appropriate site. The physical facility, including mobile units, must contain space for equipment appropriate to the services designated on the enrollment application, facilities for hand washing, adequate patient privacy accommodations, and the storage of both business records and current medical records within the office setting of the IDTF, or IDTF home office, not within the actual mobile unit.)

    - IDTF suppliers that provide services remotely and do not see beneficiaries at their practice location are exempt from providing hand washing and adequate patient privacy accommodations.

- The requirements in 42 CFR §410.33(g)(3) take precedence over the guidelines in sections 15.5.4 and 15.5.4.2 of this chapter pertaining to the supplier's practice location requirements.

- The physical location must have an address, including the suite identifier, which is recognized by the United States Postal Service (USPS).

4. Has all applicable diagnostic testing equipment available at the physical site excluding portable diagnostic testing equipment. The IDTF must—

   (i) Maintain a catalog of portable diagnostic equipment, including diagnostic testing equipment serial numbers, at the physical site;

   (ii) Make portable diagnostic testing equipment available for inspection within 2 business days of a CMS inspection request; and

   (iii) Maintain a current inventory of the diagnostic testing equipment, including serial and registration numbers, and provide this information to the designated fee-for- service contractor upon request, and notify the contractor of any changes in equipment within 90 days.

5. Maintain a primary business phone under the name of the designated business. The IDTF must have its--

   (i) Primary business phone located at the designated site of the business or within the home office of the mobile IDTF units.

   (ii) Telephone or toll free telephone numbers available in a local directory and through directory assistance.

   The requirements in 42 CFR §410.33(g)(5) take precedence over the guidelines in sections 15.5.4 and 15.5.4.2 of this chapter regarding the supplier's telephone requirements.

   IDTFs may not use "call forwarding" or an answering service as their primary method of receiving calls from beneficiaries during posted operating hours.

6. Have a comprehensive liability insurance policy of at least $300,000 per location that covers both the place of business and all customers and employees of the IDTF. The policy must be carried by a non-relative-owned company. Failure to maintain required insurance at all times will result in revocation of the IDTF's billing privileges retroactive to the date the insurance lapsed. IDTF suppliers are responsible for providing the contact information for the issuing insurance agent and the underwriter. In addition, the IDTF must--

   (i) Ensure that the insurance policy must remain in force at all times and provide coverage of at least $300,000 per incident; and

   (ii) Notify the CMS designated contractor in writing of any policy changes or cancellations.

7. Agree not to directly solicit patients; this includes - but is not limited to - a prohibition on telephone, computer, or in-person contacts. The IDTF must accept only those patients referred for diagnostic testing by an attending physician who: (a) is furnishing a consultation or treating a beneficiary for a specific medical problem, and (2) uses the results in the management of the beneficiary's specific medical problem. Non-physician practitioners may order tests as set forth in §410.32(a)(3).

   - By the signature of the authorized official in section 15 of the Form CMS-855B, the IDTF agrees to comply with 42 CFR §410.33(g)(7).

- The supplier is prohibited from directly contacting any individual beneficiary for the purpose of soliciting business for the IDTF. This includes contacting the individual beneficiary by telephone or via door-to-door sales.

- There is no prohibition on television, radio or Internet advertisements, mass mailings, or similar efforts to attract potential clients to an IDTF.

- If the contractor determines that an IDTF is violating this standard, the contractor should notify its Provider Enrollment Operations Group (PEOG) liaison immediately.

8. Answer, document, and maintain documentation of a beneficiary's written clinical complaint at the physical site of the IDTF. (For mobile IDTFs, this documentation would be stored at their home office.) This includes, but is not limited to, the following:

   (i) The name, address, telephone number, and *Medicare beneficiary identifier* of the beneficiary.

   (ii) The date the complaint was received; the name of the person receiving the complaint; and a summary of actions taken to resolve the complaint.

   (iii) If an investigation was not conducted, the name of the person making the decision and the reason for the decision.

9. Openly post these standards for review by patients and the public.

10. Disclose to the government any person having ownership, financial, or control interest or any other legal interest in the supplier at the time of enrollment or within 30 days of a change.

11. Have its testing equipment calibrated and maintained per equipment instructions and in compliance with applicable manufacturers' suggested maintenance and calibration standards.

12. Have technical staff on duty with the appropriate credentials to perform tests. The IDTF must be able to produce the applicable Federal or State licenses or certifications of the individuals performing these services.

13. Have proper medical record storage and be able to retrieve medical records upon request from CMS or its fee-for-service contractor within 2 business days.

14. Permit CMS, including its agents, or its designated fee-for-service contractors, to conduct unannounced, on-site inspections to confirm the IDTF's compliance with these standards. The IDTF must---

   (i) Be accessible during regular business hours to CMS and beneficiaries; and

   (ii) Maintain a visible sign posting its normal business hours.

15. Enrolls in Medicare for any diagnostic testing services that it furnishes to a Medicare beneficiary, regardless of whether the service is furnished in a mobile or fixed-base location.

16 Bills for all mobile diagnostic services that are furnished to a Medicare beneficiary, unless the mobile diagnostic service is part of a service provided under arrangement as described in section 1861(w)(1) of the Act. (Section 1861(w)(1) states that the term "arrangements" is limited to arrangements under which receipt of payments by the hospital, critical access hospital, skilled nursing facility, home health agency or hospice program (whether in its own right or as an agent), with respect to services for which an individual is entitled to have payment made under this title, discharges the liability of such individual or any other person to pay for the services.)

If the IDTF claims that it is furnishing services under arrangement as described in section 1861(w)(1), the IDTF must provide documentation of such with its initial or revalidation Form CMS-855 application.

The IDTF must meet all of the standards in 42 CFR §410.33 – as well as all other Federal and State statutory and regulatory requirements – in order to be enrolled in, and to maintain its enrollment in, the Medicare program. Failure to meet any of the standards in 42 CFR §410.33 or any other applicable requirements will result in the denial of the supplier's Form CMS-855 application or, if the supplier is already enrolled in Medicare, the revocation of its Medicare billing privileges.

B. Sharing of Space and Equipment

Effective January 1, 2008, with the exception of hospital-based and mobile IDTFs, a fixed-base IDTF does not: (i) share a practice location with another Medicare-enrolled individual or organization; (ii) lease or sublease its operations or its practice location to another Medicare-enrolled individual or organization; or (iii) share diagnostic testing equipment used in the initial diagnostic test with another Medicare-enrolled individual or organization. (See 42 CFR §410.33(g)(15).)

If the contractor determines that an IDTF is leasing or subleasing its operations to another organization or individual, the contractor shall revoke the supplier's Medicare billing privileges.

C. One Enrollment per Practice Location

An IDTF must separately enroll each of its practice locations (with the exception of locations that are used solely as warehouses or repair facilities). This means that an enrolling IDTF can only have one practice location on its Form CMS-855B enrollment application; thus, if an IDTF is adding a practice location to its existing enrollment, it must submit a new, complete Form CMS-855B application for that location and have that location undergo a separate site visit. Also, each of the IDTF's mobile units must enroll separately. Consequently, if a fixed IDTF site also contains a mobile unit, the mobile unit must enroll separately from the fixed location.

Each separately enrolled practice location of the IDTF must meet all applicable IDTF requirements. The location's failure to comply with any of these requirements will result in the revocation of its Medicare billing privileges.

D. Effective Date of Billing Privileges

The filing date of an IDTF Medicare enrollment application is the date that the contractor receives a signed application that it is able to process to approval. (See 42 CFR §410.33(i).) The effective date of billing privileges for a newly enrolled IDTF is the later of the following:

(1) The filing date of the Medicare enrollment application that was subsequently approved by a Medicare fee-for-service contractor; or

(2) The date the IDTF first started furnishing services at its new practice location.

A newly-enrolled IDTF, therefore, may not receive reimbursement for services furnished before the effective date of billing privileges.

The contractor shall note that if it rejects an IDTF application and a new application is later submitted, the date of filing is the date the contractor receives the new enrollment application.

E. Leasing and Staffing

For purposes of the provisions in 42 CFR §410.33, a "mobile IDTF" does not include entities that lease or contract with a Medicare enrolled provider or supplier to provide: (1) diagnostic testing equipment; (2) non-

physician personnel described in 42 CFR §410.33(c); or (3) diagnostic testing equipment and non-physician personnel described in 42 CFR §410.33(c). This is because the provider/supplier is responsible for providing the appropriate level of physician supervision for the diagnostic testing.

15.21.7.1 – Claims against Surety Bonds

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

Pursuant to 42 CFR §424.57(d)(5)(i), the surety must pay CMS - within 30 days of receiving written notice to do so - the following amounts up to the full penal sum of the bond:

(1) The amount of any unpaid claim, plus accrued interest, for which the supplier of durable medical equipment, prosthetics, orthotics and supplies (DMEPOS) is responsible.

(2) The amount of any unpaid claim, civil monetary penalty (CMP) or assessment imposed by CMS or the Office of Inspector General (OIG) on the DMEPOS supplier, plus accrued interest.

This section 15.21.7.1 describes the procedures involved in making a claim against a surety bond.

A. Unpaid Claims

1. Background

For purposes of the surety bond requirement, 42 CFR §424.57(a) defines an “unpaid claim” as an overpayment (including accrued interest, as applicable) made by the Medicare program to the DMEPOS supplier for which the supplier is responsible.

The policies in this section 15.21.7.1(A) only apply to overpayment determinations relating to services performed on or after March 3, 2009. A surety is liable for any overpayments based on dates of service occurring during the term of the surety bond. (For purposes of determining surety liability, the date of service is the date on which the service was performed/furnished.) Even if the overpayment determination is made after the expiration of the surety bond, the surety remains liable if the date of service was within the surety bond coverage period. In short, the date of service--rather than the date of the overpayment determination or the date the overpayment or demand letter was sent to the supplier---is the principal factor in ascertaining surety liability.

As an illustration, assume that a supplier has a surety bond with Company X on August 1, 2015. It performs a service on October 1, 2015. The supplier ends its coverage with Company X effective January 1, 2016 and obtains a new surety bond with Company Y effective that same date. On February 1, 2016, CMS determines that the October 1, 2015 service resulted in an overpayment; on March 2, 2016, CMS sends an overpayment demand letter to the supplier. While the overpayment determination and the sending of the demand letter occurred during Company Y’s coverage period, the date of service was within the Company X coverage period. Thus, liability (and responsibility for payment) rests with Company X, even though the supplier no longer has a surety bond with X.

2. Collection

a. Delinquency Period

If the Durable Medical Equipment Medicare Administrative Contractor (DME MAC) determines – in

accordance with CMS's existing procedures for making overpayment determinations - that (1) the DMEPOS supplier has an unpaid claim for which it is liable, and (2) no waiver of recovery under the provisions of Section 1870 of the Social Security Act is warranted, the DME MAC shall attempt to recover the overpayment in accordance with the instructions in CMS Pub. 100-06, Chapter 4.

If 80 days have passed since the initial demand letter was sent to the DMEPOS supplier and full payment has not been received, the DME MAC shall attempt to recover the overpayment. The DME MAC shall review the "List of Bonded Suppliers" the last week of each month to determine which suppliers that have exceeded this 80-day period have a surety bond. Said list:

- Will be electronically sent to the DME MACs by the Provider Enrollment & Oversight Group on a monthly basis.

- Will be in the form of an Excel spreadsheet.

- Will contain the supplier's legal business name, tax identification number, NPI, surety bond amount and other pertinent information.

If the supplier does not have a surety bond (i.e., is exempt from the surety bond requirement), the DME MAC shall continue to follow the instructions in Pub. 100-06, chapter 4 regarding collection of the overpayment.

b. Request for Payment from Surety

If, however, the supplier has a surety bond (and subject to situations (1) through (6) below), the DME MAC shall send an "Intent to Refer" (ITR) letter to the supplier and a copy thereof to the supplier's surety. The letter and copy shall be sent (a) on the same date and (b) between 80 and 90 days after the initial demand letter was sent. (The copy to the surety can be sent via mail, e-mail, or fax.)

(NOTE: Under federal law, a delinquent debt must be referred to the Department of Treasury within 120 days. (Per the chart below, this represents Day 150 of the entire collection cycle.) To ensure that the DME MAC meets this 120-day limit yet has sufficient time to prepare the surety letter as described in the following paragraph, it is recommended that the DME MAC send the ITR letter several days prior to the 90-day limit referenced in the previous paragraph. This will give the DME MAC a few additional days beyond the 30-day deadline referenced in the next paragraph to send the surety letter.)

If the DME MAC does not receive full payment from the supplier within 30 days of sending the ITR letter (and subject to situations (1) through (6) below), the contractor shall notify the surety via letter that in accordance with 42 CFR §424.57(d)(5)(i)(A), the surety must make payment of the claim to CMS within 30 days from the date of the surety letter. (The DME MAC shall send a copy of the surety letter to the supplier on the same date.) The DME MAC shall send the surety letter no later than 30 days after sending the ITR letter (subject to the previous paragraph), depending on the facts of the case. Consider the following situations:

(1) If a DMEPOS supplier has withdrawn from Medicare or has had its enrollment deactivated or revoked, the contractor shall send the ITR and the surety letter on the earliest possible days.

(2) If the supplier has an extended repayment schedule (ERS) and is currently making payments, the DME MAC shall not send an ITR letter or a surety letter. If the DME MAC is currently reviewing an ERS application from the supplier, the contractor shall delay sending the ITR letter and the surety letter until after the ERS review is complete.

(3) If the aggregated principal balance of the debt is less than $25, the DME MAC shall not send an ITR letter or a surety letter. It shall instead follow the instructions in CMS Pub. 100-06, chapter 4 regarding collection of the overpayment.

(4) If the DME MAC believes the debt will be collected through recoupment, it shall not send an ITR letter or a surety letter. It shall instead follow the instructions in Pub. 100-06, chapter 4 regarding collection of the overpayment.

(5) If the supplier has had a recent offset, the DME MAC may wait to see if future offsets will close the debt, without sending the surety a letter. If the debt is still not paid in full or an ERS has not been established, the DME MAC shall send the surety letter no later than the 115th day after the initial demand letter was sent.

(6) A payment demand letter shall not be sent to the surety if the DME MAC is certain that the $50,000 surety bond amount in question has been completely exhausted.

The DME MAC may choose to aggregate debts from the same supplier into one surety letter, provided they are at least 30 days delinquent.

The surety letter shall:

- Follow the format of the applicable model letter in section 15.21.7.1.1 of this chapter.

- Identify the specific amount to be paid and be accompanied by "sufficient evidence" of the unpaid claim. "Sufficient evidence" is defined in 42 CFR §424.57(a) as documents that CMS may supply to the DMEPOS supplier's surety to establish that the supplier had received Medicare funds in excess of the amount due and payable under the statute and regulations.

- Be accompanied by the following documents, which constitute "sufficient evidence" for purposes of §424.57(a):

(1) A computer-generated "Overpayment Services Report" containing the following information:

(i) Date of service (i.e., the date the service was furnished/performed, not the date of the overpayment determination or the date of the overpayment or demand letter)
(ii) Date on which supplier was paid
(iii) Code for type of service
(iv) Billed Amount
(v) Allowed Amount
(vi) Deductible Amount
(vii) Co-Insurance Amount
(viii) Paid Amount
(ix) Overpayment Amount

(NOTE: The report shall not include beneficiary name, *Medicare beneficiary identifier*, or any information otherwise protected under the Privacy Act.)

(2) A copy of the overpayment determination letter that was sent to the supplier.

- State that payment shall be made via check or money order and that the Payee shall be the DME MAC.

- Identify the address to which payment shall be sent.

The DME MAC shall only seek repayment up to the full penal sum amount of the surety bond. Thus, if the supplier has a $60,000 unpaid claim and the amount of the supplier's bond coverage is $50,000, the DME MAC shall only seek the $50,000 amount. The remaining $10,000 will have to be obtained from the supplier via the existing overpayment collection process.

c. Follow-Up Contact

Between 8 and 12 calendar days after sending the surety letter, the DME MAC shall contact the surety by telephone or e-mail to determine whether the surety received the letter and, if it did, whether and when payment will be forthcoming.

If the surety indicates that it did not receive the letter, the DME MAC shall immediately fax or e-mail a copy of the letter to the surety. The surety will have 30 days from the original date of the letter – not 30 days from the date the letter was resent to the surety – to submit payment. To illustrate, suppose the DME MAC on April 1 sends the surety letter, which is also dated April 1. It places the follow-up call to the surety on April 11. The surety states that it never received the letter, so the contractor e-mails a copy of it to the surety that same day. Payment must be received by May 1, or 30 days from the original date of the letter.

If the surety cannot be reached (including situations where a voicemail message must be left) or if the surety indicates that it did receive the letter and that payment is forthcoming, no further action by the contractor is required. If the surety indicates that payment is not forthcoming, the contractor shall (1) attempt to ascertain the reason, and (2) follow the steps outlined in section (A)(3)(b) below after the 30-day period expires.

The contractor shall document any attempts to contact the surety by telephone and the content of any resultant conversations with the surety.

3. Verification of Payment

a. Full Payment of the Claim Is Made

If full payment (including interest, as applicable) is made within the aforementioned 30-day period, the DME MAC shall, no later than 10 calendar days after payment was made:

(i) Update all applicable records to reflect that payment was made. (Payment from the surety shall be treated as payment from the supplier for purposes of said record updates.)

(ii) Send a mailed, faxed, or (preferably) e-mailed letter to the supplier (on which the NSC shall be copied):

- Stating that payment has been made, the date the payment was received, and the amount of the payment

- Containing the following quoted verbiage:

  "You must, within 30 calendar days of the date of this letter, obtain and submit to the NSC additional surety bond coverage in the amount of (insert the amount that the surety paid) so as to ensure that your total coverage equals or exceeds the required $50,000 amount" (or higher if an elevated bond amount is involved due to a final adverse action). "**Failure to timely do so will result in the revocation of your Medicare enrollment**.

  "Additional surety bond coverage may be obtained by (1) adding to the amount of your existing surety bond so as to equal or exceed $50,000, or (2) cancelling your current surety bond and securing a new $50,000 surety bond. (Obtaining a separate (insert the amount the surety paid) surety bond is impermissible.) In either case, the effective date of the additional coverage must be on or before the date that you submit the additional coverage to the NSC.

If the NSC does not receive the additional bond coverage within this 30-day period, it shall revoke the DMEPOS supplier's Medicare enrollment under § 424.535(a)(1) in accordance with existing procedures. (The effective date of revocation shall be the date on which the DME MAC received payment from the surety.) It is important that the NSC (1) monitor the supplier's surety bond status upon receiving a copy of

the DME MAC's letter to the supplier and (2) take prompt action against the supplier (consistent with existing procedures) if the supplier does not secure and timely submit the required additional coverage.

b. No Payment of the Claim Is Made

If the surety fails to make any payment within 30 calendar days of the date of the letter to the surety, the DME MAC shall:

(i) Refer the debt to the Department of Treasury immediately upon the expiration of said 30-day timeframe (i.e., preferably on the same day or the day after, but in all cases no later than the 120-day deadline for sending delinquent debts to the Department of Treasury) and as outlined in Pub. 100-06, chapter 4;

(ii) No later than 14 days after the 30-day period expires, contact the surety via e-mail or telephone to ascertain the reason for non-payment. Only one contact is necessary. A voice mail message may be left. The contractor shall document any attempts to contact the surety by telephone and the content of any resultant conversations with the surety.

(iii) No later than 14 days after Step (ii) has been completed – and if full payment still has not been received -- send the letter identified in section 15.21.7.1.1(E) to the surety.

(iv) Include information relating to the surety's non-payment in the report identified in section 15.21.7.1(C).

c. Partial Payment of the Claim Is Made

If the surety pays part of the claim within the 30-day period and a balance is still due and owing, the DME MAC shall do the following:

(i) Refer the unpaid debt to the Department of Treasury immediately upon the expiration of said 30-day timeframe (i.e., preferably on the same day or the day after, but in all cases no later than the 120-day deadline for sending delinquent debts to the Department of Treasury) and as outlined in Pub. 100-06, chapter 4;

(ii) No later than 14 days after the 30-day period expires, contact the surety via e-mail or telephone to ascertain the reason for the partial non-payment. Only one contact is necessary. A voice mail message may be left. The contractor shall document any attempts to contact the surety by telephone and the content of any resultant conversations with the surety.

(iii) No later than 14 days after Step (ii) has been completed – and if full payment still has not been received -- send the letter identified in section 15.21.7.1.1(E) to the surety.

(iv) Include information relating to the surety's partial non-payment in the report identified in section 15.21.7.1(C).

(v) No later than 10 calendar days after the partial payment was made:

- Update all applicable records to reflect that partial payment was made. (Payment from the surety shall be treated as payment from the supplier for purposes of said record updates.)

- Send a mailed, faxed, or (preferably) e-mailed letter to the supplier (on which the NSC shall be copied):

    - Stating that partial payment was made, the date the payment was received, and the amount of said payment

- Containing the following quoted verbiage:

"You must, within 30 calendar days of the date of this letter, obtain and submit to the NSC additional surety bond coverage in the amount of (insert the amount that the surety paid) so as to ensure that your total coverage equals or exceeds the required $50,000 amount" (or higher if an elevated bond amount is involved due to a final adverse action). "**Failure to timely do so will result in the revocation of your Medicare enrollment**.

"Additional surety bond coverage may be obtained by (1) adding to the amount of your existing surety bond so as to equal or exceed $50,000, or (2) cancelling your current surety bond and securing a new $50,000 surety bond. (Obtaining a separate (insert the amount the surety paid) surety bond is impermissible.) In either case, the effective date of the additional coverage must be on or before the date that you submit the additional coverage to the NSC."

If the NSC does not receive the additional bond coverage within this 30-day period, it shall revoke the DMEPOS supplier's Medicare enrollment under § 424.535(a)(1) in accordance with existing procedures. (The effective date of revocation shall be the date on which the DME MAC received payment from the surety.) It is important that the NSC (1) monitor the supplier's surety bond status upon receiving a copy of the DME MAC's letter to the supplier and (2) take prompt action against the supplier (consistent with existing procedures) if the supplier does not secure and timely submit the required additional coverage.

d. Successful Appeal

If the supplier successfully appeals the overpayment and the surety has already made payment to the DME MAC on the overpayment, the DME MAC shall – within 30 calendar days of receiving notice of the successful appeal - notify the surety via letter of the successful appeal and repay the surety via check or money order.

4. Summary

The following chart outlines the timeframes involved in the surety bond collection process for overpayments:

Day 1	Initial Demand Letter Sent
Day 31	Debt is Delinquent/Interest Starts
Day 41	Recoupment Starts
Day 90	Intent to Refer Letter Sent
Day 120	Surety Bond Letter Sent
Day 150	Referral to Treasury

B. Assessments and CMPs

1. Request for Payment from Surety

Per 42 CFR §424.57(a), an assessment is defined as a "sum certain that CMS or the OIG may assess against a DMEPOS supplier under Titles XI, XVIII, or XXI of the Social Security Act." Under 42 CFR §424.57(a), a CMP is defined as a sum that CMS has the authority, as implemented by 42 CFR § 402.1(c) (or the OIG has the authority, under section 1128A of the Act or 42 CFR Part 1003) to impose on a supplier as a penalty.

CMS will notify the DME MAC of the need for the latter to collect payment from the surety on an assessment or CMP imposed against a particular bonded DMEPOS supplier. Upon receipt of this notification, the DME MAC shall – regardless of the amount of the assessment or CMP - notify the surety via letter that, in accordance with 42 CFR §424.57(d)(5)(i)(B), payment of the assessment or CMP must be made within 30 calendar days from the date of the letter. The letter (on which the NSC and the supplier/debtor shall be copied) shall:

- Follow the format of the applicable model letter in section 15.21.7.1.1 of this chapter.

- Identify the specific amount to be paid and be accompanied by "sufficient evidence." This includes all documentation that CMS (in its notification to the DME MAC as described above) requests the DME MAC to include with the letter (e.g., OIG letter).

- State that payment shall be made via check or money order and that the Payee shall be CMS.

- Identify the address to which payment shall be sent.

2. Follow-Up Contact

Between 8 and 12 calendar days after sending the surety letter, the DME MAC shall contact the surety by telephone or e-mail to determine whether the surety received the letter and, if it did, whether and when payment is forthcoming;

If the surety indicates that it did not receive the letter, the DME MAC shall immediately fax or e-mail a copy of the letter to the surety. The surety will have 30 days from the original date of the letter – not 30 days from the date the letter was resent to the surety – to submit payment. To illustrate, suppose the DME MAC on April 1 sends the surety letter, which is also dated April 1. It places the follow-up call to the surety on April 11. The surety states that it never received the letter, so the contractor e-mails a copy of it to the surety that same day. Payment must be received by May 1, or 30 days from the original date of the letter.

If the surety cannot be reached (including situations where a voicemail message must be left) or if the surety indicates that it received the letter and that payment is forthcoming, no further action by the contractor is required. If the surety indicates that payment is not forthcoming, the contractor shall (1) attempt to ascertain the reason, and (2) follow the steps outlined in section (A)(3)(b) below after the 30-day period expires.

The contractor shall document any attempts to contact the surety by telephone and the content of any resultant conversations with the surety.

3. Verification of Payment

a. Full Payment Is Made

If full payment (including interest, as applicable) is made within 30 calendar days of the date of the letter to the surety, the DME MAC shall, no later than 10 calendar days after payment was made:

(i) Update all applicable records to reflect that payment was made. (Payment from the surety shall be treated as payment from the supplier for purposes of said record updates.)

(ii) Notify the applicable CMS Regional Office (RO) via letter or e-mail that payment was made.

(iii) If the OIG imposed the CMP or assessment, notify the OIG via letter that payment was made.

(iv) Send a mailed, faxed, or (preferably) e-mailed letter to the supplier (on which the NSC shall be copied):

- Stating that payment has been made, the date the payment was received, and the amount of said payment

- Containing the following quoted verbiage:

"You <u>must</u>, within 30 calendar days of the date of this letter, obtain and submit to the NSC additional surety bond coverage in the amount of (insert the amount that the surety paid) so as to

ensure that your total coverage equals or exceeds the required $50,000 amount" (or higher if an elevated bond amount is involved due to a final adverse action). "**Failure to timely do so will result in the revocation of your Medicare enrollment**.

"Additional surety bond coverage may be obtained by (1) adding to the amount of your existing surety bond so as to equal or exceed $50,000, or (2) cancelling your current surety bond and securing a new $50,000 surety bond. (Obtaining a separate (insert the amount the surety paid) surety bond is impermissible.) In either case, the effective date of the additional coverage must be on or before the date that you submit the additional coverage to the NSC."

If the NSC does not receive the additional bond coverage within this 30-day period, it shall revoke the DMEPOS supplier's Medicare enrollment under § 424.535(a)(1) enrollment in accordance with existing procedures. (The effective date of revocation shall be the date on which the DME MAC received payment from the surety.) It is important that the NSC (1) monitor the supplier's surety bond status upon receiving a copy of the DME MAC's letter to the supplier and (2) take prompt action against the supplier (consistent with existing procedures) if the supplier does not secure and timely submit the required additional coverage.

b. No Payment Is Made

If the surety fails to make any payment within the aforementioned 30-day timeframe, the DME MAC shall:

(i) Continue collection efforts as outlined in Pub. 100-06, chapter 4;

(ii) No later than 14 days after the 30-day period expires, contact the surety via e-mail or telephone to ascertain the reason for non-payment. Only one contact is necessary. A voice mail message may be left. The contractor shall document any attempts to contact the surety by telephone and the content of any resultant conversations with the surety.

(iii) No later than 14 days after Step 2 has been completed – and if full payment still has not been received -- send the letter identified in section 15.21.7.1.1(E) to the surety.

(iv) Include information relating to the surety's non-payment in the report outlined in section 15.21.7.1(C).

c. Partial Payment of the Claim Is Made

If the surety pays part of the claim within the 30-day period and a balance is still due and owing, the DME MAC shall do the following:

(i) Continue collection efforts as outlined in Pub. 100-06, chapter 4;

(ii) No later than 14 days after the 30-day period expires, contact the surety via e-mail or telephone to ascertain the reason for the partial non-payment. Only one contact is necessary. A voice mail message may be left. The contractor shall document any attempts to contact the surety by telephone and the content of any resultant conversations with the surety.

(iii) No later than 14 days after Step (ii) has been completed – and if full payment still has not been received -- send the letter identified in section 15.21.7.1.1(E) to the surety.

(iv) Include information relating to the surety's partial non-payment in the report identified in section 15.21.7.1(C).

(v) No later than 10 calendar days after the partial payment was made:

- Update all applicable records to reflect that partial payment was made. (Payment from the

surety shall be treated as payment from the supplier for purposes of said record updates.)

- Send a mailed, faxed, or (preferably) e-mailed letter to the supplier (on which the NSC shall be copied):

  - Stating that partial payment was made, the date the payment was received, and the amount of said payment

  - Containing the following quoted verbiage:

  "You must, within 30 calendar days of the date of this letter, obtain and submit to the NSC additional surety bond coverage in the amount of (insert the amount that the surety paid) so as to ensure that your total coverage equals or exceeds the required $50,000 amount" (or higher if an elevated bond amount is involved due to a final adverse action). "**Failure to timely do so will result in the revocation of your Medicare enrollment**.

  "Additional surety bond coverage may be obtained by (1) adding to the amount of your existing surety bond so as to equal or exceed $50,000, or (2) cancelling your current surety bond and securing a new $50,000 surety bond. (Obtaining a separate (insert the amount the surety paid) surety bond is impermissible.) In either case, the effective date of the additional coverage must be on or before the date that you submit the additional coverage to the NSC."

If the NSC does not receive the additional bond coverage within this 30-day period, it shall revoke the DMEPOS supplier's Medicare enrollment under §424.535(a)(1) in accordance with existing procedures. (The effective date of revocation shall be the date on which the DME MAC received payment from the surety.) It is important that the NSC (1) monitor the supplier's surety bond status upon receiving a copy of the DME MAC's letter to the supplier and (2) take prompt action against the supplier (consistent with existing procedures) if the supplier does not secure and timely submit the required additional coverage.

d. Successful Appeal

If the DMEPOS supplier successfully appeals the CMP or assessment and the surety has already made payment, CMS will – within 30 days of receiving notice of the successful appeal - notify the surety via letter of the successful appeal and repay the surety.

C. Reporting Requirements

DME MACs shall compile a report on a quarterly basis in the format prescribed in existing CMS directives. The report will capture the following elements:

- Number of account receivables (debts) reviewed for possible surety bond letter development

- Number of debts sent to the surety for recovery

- Amounts recovered directly from sureties (1) during the quarter in question, and (2) since March 3, 2009 (that is, the total/cumulative amount collected since the beginning of the surety bond collection process)

- Amounts paid by suppliers after the debt was referred to the surety for collection. The report shall include the (1) amount for the quarter in question and (2) total/cumulative amount since March 3, 2009.

- Names of suppliers and NSC numbers for which letters were sent to the surety and/or surety bond recoveries were received

- Names of suppliers on whose surety bond(s) the surety made payment in the last quarter and to whom the DME MAC consequently sent notice to the supplier that it must obtain additional surety bond coverage to reach the $50,000 threshold.

- Names and addresses of sureties that have failed to make payment within the quarterly period. For each instance of non-payment, the report shall identify (a) the amount that was requested, (b) the amount that was paid (if any), (3) the name and tax identification number of the supplier in question, and (4) the reason the surety did not pay (to the extent this can be determined).

The quarterly reports shall encompass the following time periods: January through March, April through June, July through August, and September through December. Reports shall be submitted to the Provider Enrollment & Oversight Group (with a copy to the MAC COR) --- via the following e-mail address: XXXXXXXX@cms.hhs.gov --- by the 10th day of the month following the end of the reporting quarter. Information on surety collections shall be reported once for each demand letter. That action shall be reported only when the collection process has been fully completed for that specific identified overpayment, which may be comprised of multiple claims. For example, suppose the surety was sent a letter in December but its payment was not received until January. That action would be documented in the report encompassing the months of January, February, and March.

15.27.1.2.3 – Reactivations – Miscellaneous Policies

(Rev. 876; Issued: 04-12-19; Effective: 05-13-19; Implementation: 05-13-19)

The term Medicare beneficiary identifier (Mbi) is a general term describing a beneficiary's Medicare identification number. For purposes of this manual, Medicare beneficiary identifier references both the Health Insurance Claim Number (HICN) and the Medicare Beneficiary Identifier (MBI) during the new Medicare card transition period and after for certain business areas that will continue to use the HICN as part of their processes.

A. Full Enrollment Applications

1. For providers that were deactivated for non-billing, the provider may submit a complete Form CMS-855 or Form CMS-20134 enrollment application in lieu of an RCP. The application may be submitted via paper or PECOS Web.

2. For Form CMS-855 or Form CMS-20134 reactivation applications, the timeliness requirements in sections 15.6.1 et seq., pertaining to initial enrollment applications apply. The contractor shall – unless a CMS instruction directs otherwise - validate all of the information on the application just as it would with an initial application.

3. Unless stated or indicated otherwise:

- The term “Form CMS-855 revalidations” or “Form CMS-20134 revalidations” as used in this chapter 15 only includes Form CMS-855 or Form CMS-20134 revalidation applications. It does not include RCPs.

- The term “revalidation” as used in this chapter 15 includes Form CMS-855 or Form CMS-20134 revalidation applications and RCPs.

B. Claims

For RCP submissions, the provider must also furnish a copy of a claim that it plans to submit upon the reactivation of its billing privileges. Alternatively, the provider may include in its RCP letter the following information regarding a beneficiary to whom the provider has furnished services and for whom it will submit a claim: (1) beneficiary name, (2) *Medicare beneficiary identifier (Mbi)*, (3) date of service, and (4) phone number.

C. Development

If the initial RCP is incomplete or inadequate and the contractor initiates development procedures, the following principles apply:

- The provider may submit the requested documentation to the contractor via scanned email, fax or mail.

- If there are deficiencies in the RCP letter, the provider must submit (1) a new letter, and (2) a newly-signed and dated certification statement (The certification statement may be submitted by the provider via scanned email, fax or mail). The provider cannot mark-up the previous letter and resubmit it.