Medicaid Program Integrity Manual

Appendices

Table of Contents

(Rev. 13099; Issued: 04-10-25)

Transmittals for Appendices

Appendix A

Close-Out Letter Sample

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

Date

Provider Name Attn:
Provider Address

Provider Number:
NPI Number:

Dear PROVIDER NAME:

UPIC NAME has conducted an audit on behalf of the Centers for Medicare & Medicaid Services (CMS), Medicaid Integrity Program. This audit examined claims for AUDIT ISSUE for the time period DATE through DATE.

Based upon this audit, CMS has determined no further review is necessary at this time. You should retain the records pertaining to the items and services that were the subject of this audit in accordance with applicable state and federal law (including Section 1902(a)(4) of the Social Security Act and 42 CFR 431.17). You are advised that all the claims that were the subject of this audit may be re-audited or reinvestigated at a future date by the state of STATE NAME, CMS, or other state or federal agencies or authorities.

Appendix B

Closing Summary Template

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

Medicaid Investigation/Audit Closing Summary		
Unified Program Integrity Contractor	Self-explanatory	
Jurisdiction	Self-explanatory	
UPIC Internal Tracking ID	Self-explanatory	
UCM ID	Self-explanatory	
Investigation/Audit Dates	Opened:	Closed:
State Medicaid Agency	Self-explanatory	
Provider Type	Self-explanatory	
Provider Name Provider list attachment permissible	Self-explanatory	
Provider NPI	Self-explanatory	
Description of Audit		
In this space, provide a general summary of the investigation, to include any associated allegations.		
Investigation/Audit Lead Source(s)		
In this space, provide a description of the source that prompted the opening of this investigation. Examples may be OIG, State, CPI, FPS Alert, HFPP, etc.		
Data Source		
In this space, provide a description of the data sources used during the investigation/audit. Examples may include but is not limited to TMSIS, MMIS, HFPP, State, PDMP, FQHCs, etc.		
Closure Reason		
Self-explanatory		
Next Steps		
In this space, provide a description of the next steps that may include but is not limited to referrals, 6 month look back, MFCU, education, etc.		

Additional Notes & Documentation
In this space, please provide any additional information and/or description of additional documents to be attached to this form. Examples may include separate list of related providers that could not fit in the provided fields above, provider address, citation of rules/regulations, etc.

Appendix C

Desk or Field Audit Notification Letter Sample

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

Date

Provider Name Attn:
Provider Address:
Provider Number:
NPI Number:

Dear PROVIDER NAME:

This is to inform you that you or your facility has been selected for an audit of claims billed to Medicaid with dates of services from DATE through DATE. The objective of our audit is to determine whether the claims for services were billed and paid in accordance with applicable federal and state Medicaid laws, regulations, and policies.

Section 6034 of the Deficit Reduction Act of 2005 (DRA) established the Medicaid Integrity Program, through which the Centers for Medicare & Medicaid Services (CMS) shall conduct reviews and audits of claims submitted by Medicaid providers. As a Medicaid provider and a recipient of funds under the state Medicaid program, you are subject to these reviews and audits. The DRA authorizes CMS to utilize contractors, including UPIC NAME, to conduct such reviews and audits.

In accordance with the DRA and other applicable federal laws, you are required to provide CMS and its contractor, UPIC NAME, with timely, unrestricted access to all documents and records that relate in any way to Medicaid claims and payments.

THE FOLLOWING LANGUAGE IS RELATED TO A DESK AUDIT:

To facilitate the audit, we are requesting that all documentation related to the listed claim lines on the enclosed claims listing be assembled and provided to UPIC NAME. We have included a list of types of documentation that may be required to support the claims billed. The documents must be legible and arranged in an orderly manner. Be aware that this list is not all inclusive and that UPIC NAME may request additional documentation necessary to conduct and complete its audit. The requested information should be forwarded to UPIC NAME at the following address within 30 business days from receipt of this letter.

UPIC NAME
ATTN

ADDRESS

THE FOLLOWING LANGUAGE IS RELATED TO A FIELD AUDIT:

An auditor from UPIC NAME, will be contacting you in the near future to schedule an entrance conference and discuss the audit process, which will include an on-site visit. Upon arrival at the on-site visit, UPIC NAME, will conduct an entrance conference, and will need adequate workspace to conduct the audit.
During the entrance conference, UPIC NAME, will request an overview of your organization, including your Medicaid claims submission process, any policies and procedures related to this process, and an organizational chart.

To facilitate the audit, we are requesting that certain information shown in the enclosed document be assembled and provided to UPIC NAME, at the entrance conference.

The documents must be legible and arranged in an orderly manner. This list is not all inclusive, and UPIC NAME may request additional documentation necessary to conduct and complete the audit.

Any applicable state sanctions may be imposed against you if you fail to provide the information that is requested. Depending on the laws in your state, sanctions may include, but not be limited to, vendor hold and/or exclusion from participation as a provider in the state Medicaid program, until the matter is resolved. Additionally, payments for services for which you fail to produce records to UPIC NAME will be recovered from you.

Appendix D

Medicaid Major Case Coordination Pre/Post Meeting Report – Work Details
Executive Summary Tip Sheet

(Rev.13099; Issued: 04-10-25; Effective: 05-12-25; Implementation: 05-12-25)

The Executive Summary is a free text field that the UPIC should populate to convey important information about the investigation. The information in this field should be a high-level summary of the relevant activities that have occurred during the investigation as well as any pertinent linkages and should be updated frequently. The UCM Medicaid MCC Executive Summary Tip Sheet mirrors the type of information provided in the Medicare MCC Executive Summary.

Items to Include in the Executive Summary
Allegation
A summary of the findings related to the allegation.
Background of the Investigation
Source of Data
A summary of key data findings.
A summary of investigative findings.
Detail associated with linked referring providers and/or linkages that would be of value to CMS, LE, and stakeholders.
Zone Restriction (ZR) information to include current and past ZR information.
A summary of the linkages to other investigations or suspect providers (including linkages to other UPIC/I-MEDIC investigations).
A summary of the ownership to include linkages to other entities that are of importance.
Billing company/management company information, e.g. name, etc.
Current and previous investigation information to include the date and the decisions made and the reasons why this is being presented or re-presented at the MMCC, when applicable.
Previous medical review information to include a high-level summary of the denials, denial rates, and denial reasons (identify if any of the denials were technical in nature). A summary describing if these denials are related to the same issues that are currently being investigated.
A summary of any education that was issued to the provider (including education provided by the State Medicaid Agency), including the dates the education was issued. This would include any letters that outlined corrective actions to the provider.
State Policy References
Medicare Exposure
MCO/FFS Exposure

PDMP Review (if Opioid)
Patient Harm Assessment
Dollars at Risk
Identified Medicaid Overpayment Amount
UPIC Point of Contact, including e-mail
Note: State Administration Actions are the responsibility of the state once the case is referred from the UPIC to the state or when the case was closed after it was a LE referral. Updating State Administrative Actions and outcomes in UCM is highly recommended.

Appendix E

Final Findings Report - State Transmittal Letter Template Sample

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

<Date>

<Name of State Medicaid Director>, <Title>
<Address>
<City, State, Zip Code>

Dear < Mr. /Ms. State Medicaid Director Last Name>:

Enclosed is the final findings report for <provider name>, state Medicaid provider #<number>/NPI #<number>. The investigation was conducted by <name of UPIC>, on behalf of the Centers for Medicare & Medicaid Services (CMS), and concerned Medicaid claims paid to <provider name>. The investigation encompassed the Medicaid claims <<, associated with the managed care organization <MCO name>,> for services provided during the period of <date audit period started > through <date audit period ended >.

<Name of state> is responsible for initiating the state recovery process and furnishing the final findings report to the provider. CMS will not send a copy of the final findings report to the provider. The final findings report identifies <$0,000.00> total computable, (<$0,000.00> FFP) in unallowable claims paid to <provider name>. In accordance with §1903(d)(2)(C) of the Social Security Act, <name of state> has one (1) year from the date of this letter to recover or attempt to recover the overpayment from the provider before the Federal share must be refunded to CMS. Any amounts actually collected prior to the expiration of the one year time limit, however, remain due on the CMS-64 form for the quarter in which collection is actually made (see http://www.cms.gov/smdl/downloads/SMD10014.pdf).

Please report on Line 9C1, Recoveries: Fraud, Waste and Abuse Efforts, in the amount of <$0,000.00> total computable (<$0,000.00> FFP) using feeder Form CMS-64.9C1, Line 5,

CMS Medicaid Integrity Contractors (MICs).

If you have any questions regarding this final findings report, please contact me by telephone at (312) 353-2990 or by e-mail at Elizabeth.Lindner@cms.hhs.gov.

Sincerely,

Elizabeth Lindner, Director
Division of Field Operations - North

cc: <Name of State PI Director>, <State> PI Director
<UPIC contact>
Robert Lane, CMS Division of Financial Operations, FMG, CMCS
Leticia Barraza, CMS Division of Financial Operations, FMG, CMCS
Dorothy Ferguson, CMS Division of Financial Operations, FMG, CMCS

Appendix F

Final Findings Report – State Transmittal Letter Template for FFS with No MCO Recoupment

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

<Date>

<Name of State Medicaid Director>, <Title>
<Address>
<City, State, Zip Code>

Dear < Mr. /Ms. State Medicaid Director Last Name>:

Enclosed is the final findings report for <provider name>, state Medicaid provider #<number>/NPI #<number>. The investigation was conducted by <name of UPIC>, on behalf of the Centers for Medicare & Medicaid Services (CMS), and concerned Medicaid claims paid to <provider name>. The investigation encompassed both Medicaid fee-for-service and managed care claims, associated with the managed care organization <MCO name>, for services provided during the period of <date audit period started > through <date audit period ended >.

The report identified a fee-for-service overpayment of <$0,000.00> total computable (<$0,000.00> FFP) that should be recovered by the state. The report also identified <$0,000.00> as overpayments paid by the managed care organizations; those should be handled in accordance with the state's managed care contract and the requirements of 42 CFR 438.608(d).

<Name of state> is responsible for initiating the state recovery process and furnishing the final findings report to the provider. CMS will not send a copy of the final findings report to the provider. In accordance with §1903(d)(2)(C) of the Social Security Act, <name of state>has one (1) year from the date of this letter to recover or attempt to recover the overpayment from the provider before the Federal share must be refunded to CMS. Any amounts actually collected prior to the expiration of the one year time limit, however, are due on the CMS-64 form for the quarter in which collection is actually made (see http://www.cms.gov/smdl/downloads/SMD10014.pdf).

Please report on Line 9C1, Recoveries: Fraud, Waste and Abuse Efforts, the total computable amount of <$0,000.00 amount state can recover only> (<$0,000.00 amount state can recover only> FFP). This amount should first be entered on feeder Form CMS-64.9C1, Line 5, CMS Medicaid Integrity Contractors (MICs).

If you have any questions regarding this final findings report, please contact me by telephone at (312) 353-2990 or by e-mail at Elizabeth.Lindner@cms.hhs.gov.

Sincerely,

Elizabeth Lindner, Director
Division of Field Operations - North
Investigations and Audits Group

cc: <Name of State PI Director>, <State> PI Director
<UPIC contact>
Robert Lane, CMS Division of Financial Operations, FMG, CMCS
Leticia Barraza, CMS Division of Financial Operations, FMG, CMCS
Dorothy Ferguson, CMS Division of Financial Operations, FMG, CMCS

Appendix G

Final Findings Report – State Transmittal Letter Template with No MCO Recoupment

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

<Date>

<Name of State Medicaid Director>, <Title>
<Address>
<City, State, Zip Code>

Dear < Mr. /Ms. State Medicaid Director Last Name>:

Enclosed is the final findings report for <provider name>, state Medicaid provider #<number>/NPI #<number>. The investigation was conducted by <name of UPIC>, on behalf of the Centers for Medicare & Medicaid Services (CMS), and concerned Medicaid claims paid to <provider name>. The investigation encompassed Medicaid claims associated with the managed care organization <MCO name> for services provided during the period of <date audit period started > through <date audit period ended >.

The report identified <$0,000.00> in overpayments paid by <MCO name> to the provider. This overpayment should be handled in accordance with the state's managed care contract and the requirements of 42 CFR 438.608(d). <State> is responsible for furnishing the final findings report to the provider. CMS will not send a copy of the final findings report to the provider.

If you have any questions regarding this final findings report, please contact me by telephone at (312) 353-2990 or by e-mail at Elizabeth.Lindner@cms.hhs.gov.

Sincerely,

Elizabeth Lindner, Director
Division of Field Operations - North

cc: <Name of State PI Director>, <State> PI Director
<UPIC contact>
Robert Lane, CMS Division of Financial Operations, FMG, CMCS
Leticia Barraza, CMS Division of Financial Operations, FMG, CMCS

Dorothy Ferguson, CMS Division of Financial Operations, FMG, CMCS

Appendix H

Final Findings Report Addendum – State Transmittal Letter Sample

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

<Date>

<Name of State Medicaid Director>, <Title>
<State Medicaid PI Dept. Name
<Address>
<City, State, Zip Code>

Dear < Mr. /Ms. State Medicaid Director Last Name>:

On <date FFR issued>, the Centers for Medicare & Medicaid Services (CMS) issued a final findings report for <provider name>, State Medicaid provider #<number>/NPI #<number>. The investigation was conducted by <name of UPIC> on behalf of CMS and encompassed the Medicaid claims<<,associated with the managed care organization <MCO name>,>> for services provided during the period of <date audit period started > through <date audit period ended >.

Subsequent to the issuance of the final findings report, issues relating <brief description of discrepancies identified> were discovered. Consequently, the overpayment amount on <Appendix or Attachment name >has been revised, resulting in the identified overpayment changing from <$0,000.00> to <$0,000.00>. The Federal share has changed from <$0,000.00> to <$0,000.00>.

The remainder of the above referenced final findings report shall remain unchanged and shall continue in full force and effect.

Sincerely,

Elizabeth Lindner, Director
Division of Field Operations - North

cc: <Name of State PI Director>, <State> PI Director
<UPIC contact>
Robert Lane, CMS Division of Financial Operations, FMG, CMCS
Leticia Barraza, CMS Division of Financial Operations, FMG, CMCS
Dorothy Ferguson, CMS Division of Financial Operations, FMG, CMCS

Appendix I

Information Exchange Agreement (IEA)

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

INFORMATION EXCHANGE AGREEMENT
BETWEEN

THE CENTERS FOR MEDICARE & MEDICAID SERVICES
AND

PARTICIPATING STATE MEDICAID AGENCIES
FOR

THE DISCLOSURE OF MEDICARE AND MEDICAID INFORMATION

CMS Information Exchange No. 2017-17

Effective:	
Expiration:	

I. PURPOSE, LEGAL AUTHORITY, AND DEFINITIONS

A. Purpose

The purpose of this Agreement is to establish the conditions, safeguards, and procedures under which the Centers for Medicare & Medicaid Services (CMS) will conduct an information exchange program with participating State Medicaid Agencies (SMA) that will match and study claims, billing, and eligibility information to detect suspected instances of programmatic fraud, waste and abuse (FW&A). To support the health oversight activities of CMS, CMS and the SMA and/or its contractor(s) will provide CMS and/or its contractor (hereinafter referred to as the "Custodian") with Medicare and Medicaid records pertaining to eligibility, claims, and billing information, which CMS and/or the Custodian will match.

Utilizing fraud detection software, the information will then be used to identify patternsof aberrant practices and abnormal patterns requiring further investigation. Aberrant practices and abnormal patterns identified in this matching program that constitute FW&A will involve individuals who are practitioners, providers and suppliers of services, Medicare beneficiaries, Medicaid recipients, and other individuals whose information may be maintained in the records.

Furthermore, § 6034(g) (1) (B) of the Deficit Reduction Act (DRA), Public Law (Pub.

L.aw)109-171; 42 United States Code (U.S.C.) § 1395ddd (g)(1)(B) provides for the disclosure of certain information that will be derived from these CMS health oversight activities to "States (including a Medicaid Fraud Control Unit (MFCU) described in § 1903(q))" of the Social Security Act (the Act). The SMA will therefore receive information from CMS for use in their own FW&A programs.

B. Legal Authority

This IEA is executed to comply with the Privacy Act of 1974 (Title 5 U.S.C. § 552a), as amended, and the Office of Management and Budget (OMB) Circular A-130, titled "Managing Information as a Strategic Resource" at 81 Federal Register (FR) 49689 (July28, 2016).

This Agreement provides for information exchange of matched data that is fully consistent with the authority of the Secretary of the Department of Health and Human Services (HHS) (the Secretary). Sections 1816 and 1842 of the Act permits the Secretaryto make audits of the records of providers as necessary to ensure that proper payments aremade, to assist in the application of safeguards against unnecessary utilization of servicesfurnished by providers of services and other persons to individuals entitled to benefits, and to perform other functions as are necessary (Pub. L. 108-173 § 911, amending Title XVIII, § 1874A (42 U.S.C. § 1395kk-1).

Section 1857 of the Act provides that the Secretary, or any person or organization designated by the Secretary shall have the right to "inspect or otherwise evaluate (i) thequality, appropriateness, and timeliness of services performed under the contract" (42 U.S.C. § 1395w-27(d) (2) (A)); and "audit and inspect any books and records of [a Medicare Advantage] organization that pertain to services performed or determinations ofamounts payable under the contract" (42 U.S.C. § 1395w-27(d) (2) (B)).

Furthermore, § 6402 (b) of the Affordable Care Act, which amended Title XVIII § 1860D-15(f)(2) of the Act, permits the use of Part D data "by officers, employees, and contractors of HHS for the purposes of, and to the extent necessary in conducting oversight, evaluation, and enforcement."

Additionally, § 1874(b) of the Act authorizes the Secretary to "contract with any person, agency, or institution to secure on a reimbursable basis such special data, actuarial information, and other information as may be necessary in the carrying out of his functions under Subchapter XVIII" (42 U.S.C. § 1395kk (b)).

Section 1893 of the Act establishes the Medicare Integrity Program (MIP), under which the Secretary may contract with eligible entities to conduct a variety of program safeguard activities, including fraud review employing equipment and software technologies that surpass existing capabilities (42 U.S.C. § 1395ddd)). These entities arecalled Unified Program Integrity Contractors (UPIC) and Medicare Drug Integrity Contractors (MEDIC).

Pursuant to the applicable state statutes and guidelines for the participating SMA charged

with the administration of the Medicaid program, disclosure of the Medicaid data pursuant to this Agreement is for purposes directly connected with the administration of the Medicaid program, in compliance with 42 Code of Federal Regulations (CFR) §§ 431.300 through 431.307. Those purposes include the detection, prosecution, and deterrence of FW&A in the Medicaid program. (See state signature page for the legalauthority for each specific state, if needed.)

CMS would cite to 45 CFR § 164.501 (definition of "Health Oversight Agency") and 45CFR § 164.512(d) as bases under which it believes the participating SMA may make the contemplated disclosures of Medicaid data to CMS' contractor. It would also note that under § 6034(g)(1)(B) of the DRA (42 U.S.C. 1395ddd(g)(1)(B)), CMS is required to disclose certain data and statistical information collected by the Medi-Medi program to States and other named parties. This data can then be used by each receiving state's ownFW&A programs.

C. Definitions

For purposes of this Agreement, the following definitions apply:

1. "Custodian" means the Medicaid and/or Medicare Integrity Program entity with which CMS is contracting as its Business Associate under the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules at 45 Code of Federal Regulations (CFR) Parts 160 and 164 to perform the data exchange of matched data and related functions described in this Agreement. The term Custodianshall apply to a Unified Program Integrity Contractor (UPIC) and/or the One ProgramIntegrity Systems Integrator and shall be designated on the Custodian signature page(s) of this Agreement;
2. "Medicare" means the health insurance program established under Title XVIII of theAct;
3. "Medicaid" means the Medicaid program established under Title XIX of the Act,together with other health care programs established under state law;
4. "One Program Integrity" (One PI)- Serves as a system application, tool and databasesproviding access to the CMS Integrated Data Repository (IDR) which houses, at a minimum, the most current Medicare Parts A and B billing and payment data;
5. "State Medicaid Agency" means the single State agency administering or supervisingthe administration of a State Medicaid plan.

II. DESCRIPTION OF EXCHANGE OF MATCHED DATA

The information provided by CMS on Medicare records and the participating SMA on Medicaid records will be used in an information exchange program of matched data of claimsand eligibility in the Medicare and SMA programs. CMS and the participating SMA data will be matched by linking elements of both programs that identify Medicare beneficiaries and Medicaid Program recipients as well as providers who are common to both programs. Inaddition to the provider and beneficiary/recipient identifiers, the match will

include claim data elements identifying services, procedures, diagnostic codes, prescription drugs, and other related information that may permit detection of FW&A. The exchange program of matched data described herein will be conducted via sophisticated fraud detection software that identifies patterns and deviations there-from, in data sets to identify potential FW&A.

As such, the software may match any or all fields in one record against any or all fields in one or more other records. Because of the impossibility of precisely identifying beforehand all possible matching combinations, this Agreement instead sets forth in Section III. A., a list that includes, but is not limited to, examples of data elements contained in the Medicare and Medicaid records subject to matching exchange.

In light of § 6034(g)(1)(B) of DRA, this information exchange of matched data will ultimately enhance the ability of CMS and the participating SMA to detect FW&A, as well as effectuate potential administrative actions for practitioners, providers, and suppliers in both the Medicare and Medicaid programs. Combining claims and eligibility data from multiple health programs provides a more complete picture of beneficiary/recipient care and provider practices than can be gained by analyzing data from one program in isolation and likely will reveal patterns of FW&A undetectable from analysis of data from any one particular program. This premise will be thoroughly evaluated in conducting this exchange of matched data, and to meet the DRA requirements. CMS may require additional reporting requirements from the SMA to determine the outcomes of the administrative actions identified from the matched data. To ensure adequate program evaluation, all Medicaid related reports created by the Custodian pursuant to the exchange will be provided to the participating SMA as they are provided to CMS as permitted by law.

Potential FW&A will be detected through data analysis and investigation. Identified potential FW&A in the Medicare program will be more fully developed, and referred to entities that may include the Medicare Administrative Contractors (MAC), UPIC, National Benefit Integrity (NBI), Medicare Drug Integrity Contractor (MEDIC), and/or law enforcement agencies including the HHS' Office of Inspector General, the Department of Justice, as well as other entities that are legally obligated to obtain such information. Identified potential FW&A in the State Medicaid Program detected by the exchange of matched data will be more fully developed and referred to appropriate SMA authorities, the UPIC, and/or law enforcement agencies to include both HHS' Office of Inspector General, the Department of Justice, and the SMA's Medicaid Fraud Control Unit (MFCU). Identified potential FW&A that involve both the Medicare and SMA Programs will be more fully developed and referred to the appropriate parties for further action.

III. DESCRIPTION OF RECORDS

The Privacy Act requires that each Exchange Agreement for matched data specify a description of the records which will be matched and exchanged, including a sample of data elements that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the program.

Data Elements to be used for Matching

A. Data Elements Included in Records File by the participating SMA

The participating SMA shall make available to CMS records for the matching that, at a minimum, will include the following data elements:

Recipient Identification
Recipient Identification RelationalRecipient Claim Number
Recipient Claim Number Account NumberRecipient Identification Code
Recipient Given Name Recipient Middle Name Recipient Surname NameRecipient Birth Date

Social Security Numbers
Recipient Social Security Number RelationalRecipient Social Security Number

Provider Data
Provider Identification Number (PIN) Provider National Provider Identifier (NPI)
Provider Social Security Number or Tax Identification Number

Procedure Data
HCPCS Procedure CodesCPT Procedure Codes

Diagnoses Data
ICD 9 Detail Diagnosis Code/ ICD 10 Detail Diagnosis Code (following transition)ICD 9 Primary Header Diagnosis Code/ ICD 10 Primary Header Diagnosis Code (following transition)

B. Data Elements Included in Records File by CMS

CMS shall make available records for the matching that, at a minimum, will include the following data elements:

Part A Entitlement
Beneficiary Part A Entitlement Relational Beneficiary Part A Entitlement Start Date
Beneficiary Part A Entitlement Termination DateBeneficiary Part A Entitlement Status Code

Part B Entitlement
Beneficiary Part B Entitlement Relational Beneficiary Part B Entitlement Start Date
Beneficiary Part B Entitlement Termination DateBeneficiary Part B Entitlement Status Code

Part D Entitlement
Beneficiary Part D Entitlement Relational Beneficiary Part D Entitlement Start Date
Beneficiary Part D Entitlement Termination DateBeneficiary Part D Entitlement Status Code

Entitlement Reason

Beneficiary Entitlement Reason Code Relational Beneficiary Entitlement Reason Code Change DateBeneficiary Entitlement Reason Code

Provider Data
Provider Identification Number (PIN)
Provider National Provider Identifier (NPI)
Provider Social Security Number or Tax Identification NumberDrug Enforcement Administration (DEA) number
Provider State License Identifier (if applicable)

Procedure Data
HCPCS Procedure CodesCPT Procedure Codes

Diagnoses Data
ICD 9 Detail Diagnosis Code/ ICD 10 Detail Diagnosis Code (following transition)ICD 9 Primary Header Diagnosis Code/ ICD 10 Primary Header Diagnosis Code (following transition)

Member Data
Name
Date of birthGender
SSN
SMA Member Identified

C. Disclosure of Information by CMS to the Participating SMA

The participating SMA record files will be matched against CMS files and all exchangeddata on individual recipients or providers that impact the Medicaid program will be madeavailable to the participating SMA.

D. Projected Starting and Completion Dates

The Agreement shall remain in effect for a period not to exceed 5 years from the last dateof when all parties have signed this agreement; however, within 3 months prior to the expiration of this Agreement, CMS may renew this Agreement for not more than 5 additional years subject to the requirements of the participating agencies.

E. CMS data for the Exchange of Matched Data are maintained in the Following Database:

Medicare Integrated Data Repository (IDR), System No. 09-70-0571 was published at 71FR 74915 (December 13, 2006). Data maintained in this system will be released pursuant to routine use number 11 as set forth in the system notice. The One PI Custodian will release matched data to the participating SMA. If such system infrastructure shall change then an amendment shall be added to this document to accountfor such change.

F. Number of Records Involved and Operational Time Factors

1. Medicare records will include the entire body of Medicare data for all eligible beneficiaries residing in the participating State and providers billing for treatment and services for the time period of analysis.

2. Each participating SMA's records file will contain records representing that SMA's total Medicaid utilization, as stated on the SMA signature page, related to individualswho are Medicaid recipients for the time period of analysis.

3. CMS will provide the Custodian with access to claims and eligibility data for the Medicare program updated on a monthly basis. Presently, three or more years of dataare accessible at any given time. The custodian will have access to the time period asspecified for the analysis period.

4. The participating SMA will provide the CMS with access to current Medicaid Program claims and eligibility data with updates on the frequency specified on theparticipating SMA's signature page. The participating SMA will be able to make available a minimum of 3 years of Medicaid data for FW&A analysis.

IV. RETENTION AND DESTRUCTION OF IDENTIFIABLE RECORDS

The data files provided for the data exchange program will be maintained and disclosed by CMS, and neither CMS nor the participating SMA will create a separate electronic file consisting of individuals whose records were provided in this exchange program. However, as a result of this project, files will be created for both Medicare and participating Medicaid states based on this merged data to support recovery of overpayments, or to pursue investigation and possible prosecution of fraud, waste and abuse cases. These files will be destroyed in a manner consistent with the destruction of other, similar files, created via other means. Other than files created for the aforementioned purposes, CMS and the participating SMA will retain all identifiable records received from the exchange of this matched data onlyfor the period of time required for the period of performance related to the data of this program, and will then destroy the records. Older data will be deleted as new data becomes available. Magnetic tape files shall be erased. Electronic data shall be deleted. The User agrees to destroy and send written certification of the destruction of the files to CMS within 30 days. The User agrees not to retain CMS files or any parts thereof, or specific bidding information, and those files that can be used in concert with other information to identify after the aforementioned file(s) are destroyed unless the appropriate Systems Manager or the person designated in this Agreement grants written authorization.

CMS shall maintain, acquire, use and disclose all state Medicaid data provided by the participating SMA under this Agreement in compliance with applicable laws and regulations governing such information, including but not limited to 42 U.S.C. § 1396a(a)(7), 42 CFR § 431.300 et seq., and 45 CFR § 205.50 et. seq. This responsibility includes treating all Medicaid recipient data provided by the participating SMA as confidential. CMS shall provide the participating SMA with a list of personnel authorized to access the State

Medicaid data upon request.

V. SAFEGUARDS AND SECURITY PROCEDURES

CMS has safeguards in place for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to identifiable data have been trained in the Privacy Act and information security requirements. Employees who maintain identifiable data are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

The collection of identifiable data will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations include but are not limited to: the Privacy Act of 1974; the Federal Information Security Modernization Act of 2014; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-GovernmentAct of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A-130, Managing Information as a Strategic Resource, Appendix III, and Security of Federal Automated Information Resources also applies. Federal, HHS, and CMS policies and standards include but are not limited to: all pertinent National Institute of Standards and Technology publications; and the HHS Information Systems Security and Privacy Program (IS2P).

A. CMS and the participating SMA agree to safeguard data received from each other as follows:

1. Access to the records of matched data and to any records created by the matching ofthe data exchange will be restricted to only those authorized employees and officialswho need them to perform their official duties in connection with the uses of the information authorized in this Agreement. Further, all personnel who will have access to the records of the matched data and to any records created by the matchingof the data will be advised of the confidential nature of the information, the safeguards required to protect the record and the civil and criminal sanctions for noncompliance contained in applicable Federal laws.
2. The exchanging of records of the matched data and any records created by the matching of the data will be stored in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.
3. The records of the matched data, and any records created by the matching of the data,will be processed under the immediate supervision and control of authorized personnel, to protect the confidentiality of the records in such a way that unauthorizedpersons cannot retrieve any such records by means of computer, remote terminal or other means.

4. The records of the matched data and records created by the matching of the data willbe transported under appropriate safeguards.
5. CMS may make on-site inspections, and may make other provisions to ensure that theCustodian maintains adequate safeguards. CMS shall provide the participating SMA with any reports and/or documentation relating to such on-site inspections at its request.
6. The records of the matched data and the records created by the matching of the data shall be safeguarded by administrative, physical, and technical safeguards that reasonably and appropriately protect confidentiality, integrity and availability of the data as these terms are defined in the Health Insurance Portability and AccountabilityAct (HIPAA) Security Rule at 45 CFR Parts 160 and 164. CMS shall ensure that theCustodian is in compliance with this requirement.

B. CMS and the participating SMA shall also adopt policies and procedures to ensure that information contained in their respective records shall be used solely as provided in thisAgreement.

C. CMS and the participating SMA will comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. This program of exchanging matched data employs systems which contain Protected Health Information (PHI) as defined by HHS regulation "Standards for Privacy of Individually Identifiable Health Information" (45 CFR §§ 160.103) (65 Fed. Reg. 82462 (Dec. 28, 2000)). Disclosures ofPHI authorized by the routine uses cited may only be made if, and as, permitted or required by the HIPAA Privacy Rule.

D. CMS, the data Custodian, and the participating SMA will comply with the Breach notification procedures set forth in OMB Memorandum M-17-12 "Preparing for and Responding to a Breach of Personally Identifiable Information" upon discovery by a Party to this contract of any suspected or confirmed Breach, inappropriate use of data, or Security Incident. The Party experiencing the event will notify the other agency's SystemSecurity Contact named in this Agreement within one (1) hour of discovering the loss, potential loss, Security Incident, or Breach.

If the Custodian and/or the participating SMA is unable to speak with the CMS Systems Security Contact within one hour or if for some other reason notifying the CMS Systems Security Contact is not practicable (e.g., it is outside of the normal business hours), the data Custodian and /or participating SMA will contact the CMS IT Service Desk at 410-786-2580 or e-mail CMS-IT-ServiceDesk@cms.hhs.gov.

E. The Party that experienced the loss, potential loss, Security Incident, or Breach will be responsible for following its established procedures, including notifying the proper organizations (e.g., United State Computer Emergency Readiness Team (US-CERT)), conducting a breach and risk analysis, and making a determination of the need for notice and/or remediation to individuals affected by the loss. Parties under this Agreement will follow PII Breach notification policies and related procedures

as required by OMB guidelines. If the Party experiencing the Breach determines that the risk of harm requiresnotification to the affected individuals or other remedies that Party will carry out these remedies without cost to the other Party.

The SMA agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is not less thanthe level and scope of security requirements established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems) as well as Federal Information Processing Standard 200entitled "Minimum Security Requirements for Federal Information and Information Systems"; and, Special Publication 800-53 "Recommended Security Controls for FederalInformation Systems". The SMA acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable, bidder identifiable or deducible information derived from the file(s) specified prohibited.

Further, the SMA agrees that the data must not be physically moved, transmitted or disclosed in any way from or by the site indicated in without written approval from CMSunless such movement, transmission or disclosure is required by a law.

VI. RECORDS USAGE, DUPLICATION, AND RE-DISCLOSURE RESTRICTIONS

CMS and the participating SMA agree to the following limitations on the access to and disclosure and use of, the tapes and information provided under this Agreement.

1. That the data files provided for the program of exchanging matching data will be maintained and disclosed by the CMS Custodian and will be handled as indicated in Section IV of this Agreement.
2. That the data supplied and the records created by the matching will be used and accessedonly for the purposes of, and to the extent necessary in, the program created by this Agreement.
3. That the data provided by the participating SMA will not be duplicated in a separate fileor disseminated for purposes other than those intended by this Agreement without the written consent of the participating SMA.
4. That, other than for purposes of a particular match under this program, no file will becreated that consists of information concerning only matched individuals.

VII. REIMBURSEMENT FUNDING

All work to be performed by the Custodian to carry out the exchange in accordance with this Agreement will be performed on a contractual basis by the Custodian as prescribed inthe contract between the Custodian and CMS. All work to be performed by the participating SMA to carry out the requirements of this exchange program in accordance with this Agreement will be performed on a non-reimbursable basis, except to the extent that those requirements may include administrative or other activities eligible for Federal financial participation.

VIII. APPROVAL AND DURATION OF AGREEMENT

A. Effective Date: This Information Exchange Agreement will become effective from the last date of when all parties have signed this agreement and will remain in effectfor a period not to exceed 5 years from the effective date of the Agreement. This Agreement may be renewed for consecutive 5 year periods subject to the requirements of the participating agencies. Information exchange activities will continue without interruptions during agreement renewal procedurals.

B. This Agreement may be terminated at any time with the consent of both parties. If either party does not want to continue this program, it shall notify the other party of its intention not to continue at least 90 days before the end of the then current period of the Agreement. Either party may unilaterally terminate this Agreement upon written notice to the other party requesting termination, in which case the terminationshall be effective 90 days after the date of the notice or at a later date specified in the notice provided the expiration date does not exceed the original or the extended completion date of the exchange. At such time when the agreement terminates, CMS and the SMA will determine such appropriate closeout procedures to insure the safeguard of CMS data and data obtained from the SMA. The closeout process will also bring any outstanding analysis, audits and other investigative activities to a finalstatus for transition to the applicable party.

IX. PERSONS TO CONTACT

A. The CMS contact for Programmatic issues:

Elizabeth Lindner
DFO-N Director
Division of Field Operations - NorthInvestigations and Audits Group Center for Program Integrity
Centers for Medicare and Medicaid ServicesPhone: 312-353-2990
E-mail: elizabeth.lindner@cms.hhs.gov

B. The CMS contact for Privacy issues:

Barbara Demopulos
CMS Privacy Advisor
Division of Security, Privacy Policy and GovernanceInformation Security and Privacy Group
Office of Information Technology
Centers for Medicare & Medicaid Services 7500 Security Boulevard, Mail Stop: N1-14-40
Baltimore, MD 21244-1849
Telephone: 410-786-5357

E-mail: Barbara.demopulos@cms.hhs.gov

C. The contact person for the participating SMA can be found on the SMA signature page.

D. The contact person for the Custodian can be found on the Custodian signature page.

E. The contact person for the CMS One Program Integrity Systems Integrator can be foundon the CMS One Program Integrity Systems Integrator signature page

X. APPROVALS

A. Centers for Medicare & Medicaid Services Program Official

The authorized program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, confirm that no verbal agreements ofany kind shall be binding or recognized, and hereby commits his respective organizationsto the terms of this Agreement.

Approved by (Signature of Authorized CMS Program Official)	
Print name of CMS CPI Official	**Date:**

B. Centers for Medicare & Medicaid Services Approving Official

The authorized approving official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, confirm that no verbal agreements of any kind shall be binding or recognized, and hereby commits his respective organizations to the terms of this Agreement.

Approved By (Signature of Authorized CMS Approving Official)	
Michael Pagels, Director Division of Security, Privacy Policy and Governance, andActing Senior Official for Privacy Information Security & Privacy GroupOffice of Information Technology Centers for Medicare & Medicaid Services	**Date:**

C. Participating State Program Official

The authorized Participating State program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits his/her respective organization to the terms of this Agreement.

NAME OF PARTICIPATING STATE

Approved by (Signature of Authorized State Program Official)	
Print name of Authorized State Program Official	**Date:**

The Participating State Records to Be Exchanged for Matching:

The data for the _____ that will be made available for the exchange program described herein are maintained in the following data files and the frequency of the exchange of data will be made on a monthly basis. (All or part of these files may be used in this data-exchange program):

MMIS which will submit approximately _____ of claims and _____ of encounters annually.

The type of data files being shared on a monthly basis by the

_____

shall include but is not limited to:

Claims – managed care/encounter data, crossover and TPL claims, adjustments/ voids, denied claims.

Eligibility - files that include all data elements that are associated with claim adjudication, and any retro-active eligibility activity

Provider - Medicaid files including any Medicare and NPI reference files

Participating State Legal Authority (as needed):

D. CMS Custodian Official

The authorized CMS Custodian official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein,confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits his/her respective organization to the terms of this Agreement.

Approved by (Signature of Authorized CMS Custodian Official)	
Print name of Authorized CMS Custodian Official	Date:

E. CMS One Program Integrity Systems Integrator

The authorized OptumServe Technology Services (One PI) systems support contractor official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, confirms that no verbal agreements of any kind shall be bindingor recognized, and hereby commits his/her respective organization to the terms of this Agreement.

Approved by (Signature of OptumServe Technology Services official)	
Print name of OptumServe Technology Services Official	Date:

Appendix J

Joint Operating Agreement (JOA)
((Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

Joint Operating Agreement (JOA) Between [Insert UPIC name] and [SMA name]

[Insert Date]

Change History Log

Version	Date	Changed By	Description of Change

Section 1. Introduction

[This template is a guide and includes suggested language which may be changed pending the agreement of the UPIC and the state Medicaid agency (SMA).]

1.1 Unified Program Integrity Contractor (UPIC) Purpose

The purpose of the UPIC in Medicaid is to work with SMAs to identify potential fraud, waste, and abuse across the Medicaid and Medicare programs. The program incorporates data matching, coordination, and information sharing to identify fraudulent or wasteful billing behavior that goes undetected when the programs are reviewed in isolation.

1.2 Partner Responsibilities

Medicaid program integrity is a collaborative effort between CMS, [Insert UPIC name] (under contract to CMS), [Insert SMA name], and law enforcement officials. The following table summarizes the roles and responsibilities of each partner.

CMS	[Insert SMA name]
Provide funding and oversight for the UPIC Conducts outreach to states to assess the program integrity needs Provides open forum for communication and facilitates information sharing Participate in the Initial State Collaboration Meeting and program management meetings Execute the Information Exchange Agreement Establish connectivity with SMA Provide CMS system training Provide Medicare and Medicaid policy and data assistance Participate in national-level document sharing	Participate in Initial State Collaboration Meeting Renew Information Exchange Agreement, if applicable Complete Joint Operating Agreement Establish connectivity, if needed Provide Medicaid data, if applicable Provide and participate in training Contribute to the Data Analysis Project Management Strategy Provide Medicaid policy and data assistance Participate in the Data Workgroup (if applicable) Participate in program management meetings Follow established fraud, waste, and abuse investigations, audits, and referral processes Work on joint investigations or share investigative findings Contribute to state-level and national level document sharing
[Insert UPIC name]	

Facilitate the Initial State Collaboration Meeting Establish Joint Operating Agreement Develop Data Analysis Project Management Strategy Provide and receive training Facilitate program management meetings Provide Medicare and Medicaid policy and data assistance Conduct data matching and/or data analysis Conduct fraud, waste, and abuse investigation and referral processes Work on joint investigations Contribute to state-level and national-level document sharing Participate in Data Workgroup	

1.3 Joint Operating Agreement Purpose

This Joint Operating Agreement (JOA) is an agreement between [insert UPIC name] and [insert SMA name] to establish guidelines, duties, and shared expectations of how each will conduct business with the other. This JOA will include any agreement between the SMA and the UPIC on program implementation and operation that is not specified in the PIM.

[Insert UPIC name] and [Insert Medicaid State Agency name] collaborated on the development of this JOA and agree with the terms of the agreement.

1.4 Maintaining the JOA

1.4.1 Annual Updates

The JOA should be revisited annually. The [insert UPIC name] Medicaid Operations Lead will be responsible for coordinating the review and revision process.

1.4.2 On-going Updates

All updates are to be sent to the [insert UPIC name] Medicaid Operations Lead. Within [insert number] weeks, the [insert UPIC name] Medicaid Operations Lead will distribute a draft to all points of contact identified in this JOA. Feedback is to be provided within [insert number] weeks. The [Insert UPIC name] project lead will then

distribute a final draft to all points of contact. The [Insert SMA name] contact person will provide approval of the changes via email or other written format.

1.4.2 Tracking of Changes

Changes to the JOA are identified in the Change History Log on the second page of this document and are controlled via a version number in the upper right-hand corner of each page of the document. Changes to the appendices to this document are also controlled via a version number in the upper right-hand corner of each appendix.

1.5 Liability

Although [insert UPIC name] has a contractual relationship with CMS, there is no privity of contract between [insert UPIC name] and [insert SMA name]. [Insert UPIC name] will be indemnified and protected by limitations on liability according to the terms of the [insert UPIC name]'s "[insert name of UPIC contract". [Insert UPIC name] will be indemnified and protected by limitations on liability according to the terms of its UPIC contract. [Insert UPIC name] is protected against criminal or civil liability as a result of the performance of duties as a program integrity contractor under its contract as long as it uses due care. See 63 Fed. Reg. 13,590 (1998) (to be codified at 42 C.F.R. 421.316) (proposed March 20, 1998). In light of the provisions of [insert UPIC name]'s current contract with CMS and the constraints of law, no amendments to [insert UPIC name]'s contract will be made with respect to indemnification or limitations on liability.

1.6 Guiding Documents

The [insert UPIC name] is required to adhere to applicable federal laws, regulations, the CMS Program Integrity Manual (PIM), and the Statement of Work established with CMS.

The [Insert SMA name] is required to adhere to applicable federal and state laws, and regulations.

Section 2. Implementation

This section describes the implementation of Medicaid program integrity coordination efforts in [Insert State].

2.1 Information Exchange Agreement

When applicable, the [insert SMA name] will renew the Global Information Exchange Agreement (IEA) with CMS.

Section 3. Dispute Resolution

<Describe the process for resolving disputes between the UPIC and the SMA.>

Section 4. Communications Plan

4.1 Points of Contact

To assure that communication is properly directed, [insert UPIC name] and [insert SMA name] will each identify (in the Master Contact List) representative(s) to serve as:

Medicaid Operations Lead and/or Program Integrity Manager – Responsible for acting as the main project lead for Medicare program integrity coordination efforts. The lead is responsible for establishing and maintaining the JOA and for leading the resolution of any JOA-related issues that may arise.

Data Manager – Responsible for the exchange of information regarding data analysis issues, including understanding the data sources.

[Other roles may be added as appropriate and do not necessary require the level of Key Personnel as listed in the UPIC SOW.]

4.2 Regular Collaboration

[Insert information on regular meetings that will occur between the UPIC and the SMA. Two examples are shown below.]

4.2.1 Program Management Meeting

[Insert UPIC name] and [insert SMA name] will participate in Program Management Meetings. The staff participating in the Program Management Meetings are identified in the "Master Contact" list at the end of the JOA. [Insert information on the role of the Program Management Meetings and the frequency of meetings]

4.2.2 Medicaid Program Integrity Coordination Data Workgroup

[Insert UPIC name] and [insert SMA name] will participate in a data workgroup. The staff participating in the data workgroup is identified in the Master Contact table at the end of the JOA. [Insert information on the role of the data workgroup and the frequency of meetings]

Section 5. Training and Information Sharing

[Describe how the UPIC and the SMA will provide cross-training on programs, policies, and data. See the Medicaid PIM for guidance.]

5.1 Initial Cross-Training

5.2 Ongoing Training

5.3 Subject-Matter Experts

Section 6. Connectivity and Data Sharing

6.1 Connectivity

[Insert UPIC name] and [insert SMA name] and CMS will work together to determine how data will be shared.

[Insert UPIC name] will develop an Information Technology (IT) Plan providing details about the data sharing, including security concerns. [Insert SMA name] and CMS will provide input to the IT Plan.

6.2 Data Sources

[Describe the source of Medicaid data, including the type and elements]

6.3 Reserved

6.4 Data Validation

[Insert UPIC name] is responsible for validating data to ensure program needs are met. If data are not of sufficient quality, [Insert UPIC name] will identify the problem to [Insert SMA name] and to CMS. [Insert UPIC name] and [insert SMA name] will work together through the Data Workgroup to resolve any data problems that arise.

6.5 Security - [Due to the content of this information, it may not be revised by the SMA or the UPIC.]

[Insert UPIC name] and [Insert SMA name] will meet the security requirements detailed below (of note, should the SMA have an IEA in place with the UPIC, these security requirements are also detailed in that agreement).

A. [Insert UPIC name] and the participating SMA agree to safeguard data received from each other as follows:

1. Access to the records of data will be restricted to only those authorized employees and officials who need them to perform their official duties in connection with the uses of the information authorized in this Agreement. Further, all personnel who will have access to the records of the data will be advised of the confidential nature of the information, the safeguards required to protect the record and the civil and criminal sanctions for noncompliance contained in applicable Federal laws.
2. The exchanging of records of the data will be stored in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.
3. The records of the data will be processed under the immediate supervision and control of authorized personnel, to protect the confidentiality of the records in such a way that unauthorized persons cannot retrieve any such records by means of computer, remote terminal or other means.
4. The records of the data will be transported under appropriate safeguards.
5. The records of the data shall be safeguarded by administrative, physical, and technical safeguards that reasonably and appropriately

protect confidentiality, integrity and availability of the data as these terms are defined in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule at 45 CFR Parts 160 and 164. CMS shall ensure that the Custodian is in compliance with this requirement.

B. [Insert UPIC name] and the participating SMA will comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. This program of exchanging data employs systems which contain Protected Health Information (PHI) as defined by HHS regulation "Standards for Privacy of Individually Identifiable Health Information" (45 CFR §§ 160.103) (65 Fed. Reg. 82462 (Dec. 28, 2000)). Disclosures of PHI authorized by the routine uses cited may only be made if, and as, permitted or required by the HIPAA Privacy Rule.

C. [Insert UPIC name] and the participating SMA will comply with the Breach notification procedures set forth in OMB Memorandum M-17-12 "Preparing for and Responding to a Breach of Personally Identifiable Information" upon discovery by a Party to this contract of any suspected or confirmed Breach, inappropriate use of data, or Security Incident. The Party experiencing the event will notify the other agency's System Security Contact named in this Agreement within one (1) hour of discovering the loss, potential loss, Security Incident, or Breach.

If the Custodian and/or the participating SMA is unable to speak with the CMS Systems Security Contact within one hour or if for some other reason notifying the CMS Systems Security Contact is not practicable (e.g., it is outside of the normal business hours), the data Custodian and /or participating SMA will contact the CMS IT Service Desk at 410- 786-2580 or e-mail CMS-IT-ServiceDesk@cms.hhs.gov.

D. The Party that experienced the loss, potential loss, Security Incident, or Breach will be responsible for following its established procedures, including notifying the proper organizations (e.g., United State Computer Emergency Readiness Team (US-CERT)), conducting a breach and risk analysis, and making a determination of the need for notice and/or remediation to individuals affected by the loss. Parties under this Agreement will follow PII Breach notification policies and related procedures as required by OMB guidelines. If the Party experiencing the Breach determines that the risk of harm requires notification to the affected individuals or other remedies that Party will carry out these remedies without cost to the other Party.

The SMA agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is not less than the level and scope of security requirements established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems) as well as Federal Information Processing Standard 200 entitled "Minimum Security Requirements for Federal Information and Information Systems"; and, Special Publication 800-53 "Recommended Security Controls for Federal Information Systems". The SMA acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable, bidder identifiable or deducible information derived from the file(s) specified prohibited.

Further, the SMA agrees that the data must not be physically moved, transmitted or disclosed in any way from or by the site indicated in without written approval from CMS unless such movement, transmission or disclosure is required by a law.

Section 7. Data Analysis

[Insert UPIC name] will conduct data analysis and report results of the data analysis to [insert SMA name].

7.1 Identifying and Prioritizing

[Insert UPIC name] and [insert SMA name] will contribute to the identification and prioritization of potential vulnerabilities as identified in the Policies and Procedures Manual.

[Describe how the vulnerabilities will be identified and when the prioritization will occur, i.e. through the data workgroup, through the Project Leads, or other processes.]

7.2 Data Analysis Project Management Strategy

[Insert UPIC name] will develop a Data Analysis Project Management Strategy that describes the ongoing and ad hoc analyses that will be completed each year. [Insert SMA name] will provide input to the plan.

[Describe how collaboration will occur, i.e. through the data workgroup or the Project Leads]

7.3 Data Analysis Reports

[Insert UPIC name] will adhere to the reporting requirements outlined Medicaid PIM. [Describe any requirements that are unique to the SMA regarding data analysis reports]

Section 8. Investigations and Referrals

[Insert UPIC name] will adhere to the requirements of the Program Integrity Manual (PIM) and the PPM.

[Insert SMA name] will adhere to [Insert applicable regulation document.]

[Provide a summary of the clarifications agreed to by the UPIC and the SMA on the overall strategy for working collaboratively on program integrity activities, especially those issues that might be outside of the PIM, PPM, or state regulations.]

8.1 Joint Investigations

[Describe how joint investigations will be conducted.]

8.2 Referrals

[Insert UPIC name] will refer Medicare cases per the Program Integrity Manual. [Insert SMA name] will refer cases to the [insert applicable agency] per the [insert applicable regulation document.]

[Insert any information that would be unique to the state program.]
(See Master Contact List on next page)

Master Contact

Name	Role	Title	Phone Numbers	Email	Mailing Address
[Insert UPIC name]					
[Insert SMA name]					

Appendix K

Medicaid Program Integrity Manual Acronyms

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

American Academy of Professional Coders (AAPC)
Business Function Lead (BFL)
Center for Program Integrity (CPI)
Centers for Medicare & Medicaid Services (CMS)
Certified Professional Coder (CPC)
Children's Health Insurance Program (CHIP)
Civil Monetary Penalty (CMP)
Contracting Officer's Representative (COR)
Current Procedural Terminology (CPT)
Deficit Reduction Act (DRA)
Department of Justice (DOJ)
Federal Medical Assistance Percentage (FMAP)
Federal Financial Participation (FFP)
Final Findings Report (FFR)
Initial Findings Report (IFR)
Internet Only Manual (IOM)
Local Coverage Determination (LCD)
Medicaid Fiscal Agent (MFA)
Medicaid Fraud Control Unit (MFCU)
Medical Review (MR)
National Coverage Determination (NCD)
Department of Health and Human Services - Office of Inspector General/ Office of Investigations (HHS-OIG/OI)
Program Integrity (PI)
State Medicaid Agency (SMA)
Surveillance Utilization Review Subsystem (SURS)
Umbrella Statement of Work (USOW)
Unified Program Integrity Contractor (UPIC)

Appendix L

State Collaboration Vetting Form Sample

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

Date Sent to State: Click here to enter text.

Sent to: Click here to enter text. **CC:** Click here to enter text.

Sent by: Click here to enter text.

Provider Information

Provider Name: Click here to enter text.

Provider Entity Type (LLC, Inc., etc.): Click here to enter text.

Provider Location: Click here to enter text.

Provider NPI: Click here to enter text.

Provider TPI: Click here to enter text.

Provider Medicaid ID: Click here to enter text.

ZPIC Internal Tracking Number: Click here to enter text.

Review Period: Click here to enter text.

Type of Provider: Click here to enter text.

Provider Ownership: Click here to enter text.

HHS-OIG Exclusion List: Click here to enter text.

Previous Reviews/Administrative actions taken (UPIC and/or MAC): Click here to enter text.

Prior/Current State Action:

Current or past known non-OIG State administrative actions taken: Click here to enter text.

Current or past known State OIG reviews/actions taken: Click here to enter text.

Potential Medicaid Allegations (if applicable, attach additional information to support the Medicaid peril)

Description of specific suspected behavior, Medicaid violation or scheme in this investigation:
Click here to enter text.

Medicaid Payment Requirements/Policy:

Click here to enter text.

Top Three Procedure Codes: Click here to enter text.

Medicaid Dollars at Risk Related to the Allegation: Click here to enter text.

Response from the State: (select one)

☐ The State has no interest in this provider.

Please indicated why state has no interest:

☐ The State is interested in joint collaboration and will work with the UPIC.

☐ The State requests the UPIC to develop an investigation on this provider and advise of its progress during the ongoing investigation.

☐ The State requests further information:

UPIC Contact (Name & Phone): Click here to enter text.

State Investigations Contact (Name & Phone): Click here to enter text.

State Audit Contact (Name & Phone): Click here to enter text.

State Response Date: Click here to enter text.

Additional feedback from the State: Click here to enter text.

Appendix M

Vulnerability Template

(Rev. 11948; Issued:04-13-23, Effective: 05-15-23; Implementation: 05-15-23)

Vulnerability Template Date Submitted:

Submitted By:

Name:

Organization:

Phone:

Email:

Vulnerability

Vulnerability Title:

Provider Type (if applicable):

Vulnerability Description:

Risk Factors (specific conditions, drivers, and/or actions that likely cause the vulnerability or increase the chances of it occurring):

- Be as specific as possible about what the root cause(s) of the vulnerability may be. This field provides detail that may be used to ultimately help "solve the problem" and mitigate the vulnerability.

For the below, provide risk assessment point valuation and provide a written justification for each (This is not required but will greatly assist in the vulnerability process).

Likelihood (likelihood for the identified vulnerability. Provide 1-2 sentences behind the reasoning for selecting this level of likelihood for the vulnerability):

4 - Almost Certain (≥75% likelihood to occur)
3 - Likely (≥50% - <75% likelihood to occur)
2 - Possible (≥25% - <50% likelihood to occur)
1 - Unlikely (<25% likelihood to occur)

Patient Harm (Provide 1-2 sentences behind the reasoning for selecting this level of likelihood for the vulnerability):

4 - Life Threatening
3 - Significant
2 - Minimal
1 - No harm

Financial Impact (Provide 1-2 sentences behind the reasoning for selecting this level of financial impact for the vulnerability):

4 - Greater than $200m (≥$200 million)
3 - $100m - $200m (≥$100 million <$200 million)
2 - $10m - $100m (≥$10 million ≤$100 million)
1 - Less than $10m (<$10 million)

Breadth (Provide 1-2 sentences behind the reasoning for selecting this level of breadth for the vulnerability):

4 - National
3 - Regional
2 - Pocketed
1 - Isolated

Existing Controls (Provide current projects or activities that are underway to address the risk factor):

Suggested Mitigation Activities (Suggestions for action items (i.e. key results) that may help to mitigate the risk factor(s):

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

FPS Model-Related (Y/N):

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

Attachments (If applicable, upload document(s), such as Office of Inspector General reports or relevant data that can provide additional information or context on the vulnerability being reported):

Appendix N

State Vetting Form for the Managed Care Plan Project

(Rev.13099; Issued: 04-10-25; Effective: 05-12-25; Implementation: 05-12-25)

Date Sent to State:
Sent to: CC:
Sent by:

UPIC Contact (Name & Phone):

Plan Information
Managed Care Plan Name:
Plan Type (MCO, PIHP, PAHP):
Plan Location:
Plan NPI (if applicable):
Plan Medicaid ID(s):
Plan Ownership:
HHS-OIG Exclusion List:

Review Information
Review Period:
Areas to be covered include, but are not limited to:

- *Capitation payments*
- *Program Integrity Activities*
- *Payments to network providers*
- *Reviewing denied claims*
- *Reviewing denied prior authorizations*
- *Provider Network Adequacy*
- *Providing Preventive Services*

Prior/Current State Action:

1. *Have there been any audits or reviews of the plan or its network in the past two Federal Fiscal Years?*
   If so, please list the areas of review/audit and the period covered:
2. *Current or past State administrative actions taken:*
3. *Current or past State MFCU reviews/actions taken:*

Response from the State: (select one)
☐ *The plan is cleared to move forward for the UPIC's review.*
☐ *The plan is NOT cleared to move forward for the UPIC's review due to:*

State Investigations Contact (Name & Phone):
State Audit Contact (Name & Phone):
State Response Date:

Transmittals Issued for this Chapter

Rev #	Issue Date	Subject	Impl Date	CR#
R13099MPI	04/10/2025	Updates of Appendices in Publication (Pub.) 100-15, Including Formatting Edits and Addition of State Vetting Form for the Managed Care Plan Project	05/12/2025	13931
R12871MPI	10/11/2024	Updates of Chapter 1, Chapter 2, Chapter 3, Chapter 4, and Appendices in Publication (Pub.) 100-15, Including Auditing of Program Integrity Activities in Managed Care Plans	11/14/2024	13720
R11948MP	04/13/2023	Updates of Publication (Pub.) 100-15, Including Revisions to Chapters 1 and 2, and the Addition of Chapters 3, 4, 5, and Appendices	05/15/2023	13141

Back to top of Chapter