

**INFORMATION EXCHANGE AGREEMENT
BETWEEN
CENTERS FOR MEDICARE & MEDICAID SERVICES
AND
THE PARTICIPATING MEDICAID AGENCY
FOR THE
DISCLOSURE AND EXCHANGE OF CERTAIN MEDICARE AND MEDICAID
DATA
OF DUALY ELIGIBLE INDIVIDUALS**

CMS AGREEMENT No. 2025-50

I. PURPOSE, LEGAL AUTHORITIES, AND DEFINITIONS

A. Purpose

This Information Exchange Agreement (IEA), hereinafter the “Agreement,” establishes the terms, conditions, safeguards, and procedures under which the Centers for Medicare & Medicaid Services (CMS) and the undersigned state (through or on behalf of the agency that operates the state's Medicaid plan – hereinafter the "Participating Medicaid Agency" (PMA)) will exchange certain Personally Identifiable Information (PII) and Protected Health Information (PHI) from CMS Data regarding beneficiaries dually eligible for Medicare and Medicaid (“Dually Eligible Beneficiaries” or “Dually Eligible Individuals”), for the purpose of the administration of a number of programs for Dually Eligible Individuals for the [insert name of state]’s Medicaid agency. This Agreement and the corresponding Data Request Attestation (DRA) document the PMA’s assertions regarding its legal authority to request and receive such data, as well as the terms, conditions, safeguards, and procedures CMS imposes on the PMA as a condition of the PMA’s receipt of such data.

When executed, this Agreement, along with the corresponding DRA, will offer a PMA a single streamlined data request process for such CMS Data, including opportunities to request certain elective data files, as well as the means of carrying out operational data exchanges that support the dually eligible population. These activities are described more fully in Section III.A. of this Agreement. This data request process will be managed by CMS’ Federal Coordinated Health Care Office (known as the “Medicare-Medicaid Coordinated Office” or “MMCO”).

The elective data files and exchange programs may include, but are not limited to, the Territory & State Beneficiary Query (TBQ) File¹ and the data files shared under the

¹ See <https://www.cms.gov/data-research/research/statistical-resources-dually-eligible-beneficiaries/territories-states-beneficiary-query-tbq-file>.

Medicare-Medicaid Data Sharing Program.² The operational exchanges are the data exchanged for the State Buy-In File Exchange³ and the Medicare Modernization Act File Exchange.⁴

CMS and the PMA are each a “Party,” and, collectively, “the Parties,” to this Agreement. By entering into this Agreement, the Parties agree to comply with the terms and conditions set forth herein, as well as applicable law and regulations. The terms and conditions of this Agreement will be carried out by authorized officers, employees, and contractors of CMS and the PMA.

This Agreement does not constitute a computer matching agreement governing a “matching program” as defined by the Privacy Act of 1974 (5 U.S.C. § 552a(a)(8)) because, though it does contemplate the computerized comparison of two or more automated systems of records or a system of records with non-Federal records, it will not be for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or recouping payments or delinquent debts under such Federal benefit programs.

Any disclosure(s) of CMS Data, or any individually-identifiable derivative of this CMS Data, by the undersigned or its agents to a Downstream User, as defined below, shall be made in accordance with applicable law as well as any applicable provisions in this or other governing documents.

B. Legal Authorities

The following statutes and regulations govern the exchange and/or disclosure of CMS Data under this Agreement and the corresponding DRA:

1. CMS:

- a. The Privacy Act of 1974 (5 U.S.C. § 552a), and the regulations and guidance promulgated thereunder;
- b. Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, that appears at 81 Federal Register (FR) 49689 (July 28, 2016).

² See <https://www.cms.gov/data-research/research/statistical-resources-dually-eligible-beneficiaries/state-access-medicare-data>.

³ See Chapter 2 of the Manual for State Payment of Medicare Premiums at <https://www.cms.gov/medicare/medicaid-coordination/about/state-payment-premiums>.

⁴ See <https://www.cms.gov/data-research/research/statistical-resources-dually-eligible-beneficiaries/state-mma-file-dual-eligible-beneficiaries>.

- c. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules at 45 Code of Federal Regulations (CFR) parts 160 and 164.
 - d. Section 2602 of Public Law (P.L.) 111-148, which addresses CMS responsibilities including providing states with the tools necessary to develop programs to align Medicare and Medicaid benefits for Dually Eligible Individuals (not applicable to territories).
 - e. Section 1106(a) of the Social Security Act (the Act), which permits the disclosure of U.S. Department of Health and Human Services (HHS) agency data where such disclosures are authorized by statute or regulation.
 - f. Sections 1843 and 1818(g) of the Act, and the implementing regulations at 42 CFR § 407.40 et seq., and § 406.26 which require the Secretary of HHS to enter into a State Buy-in agreement at the request of any state or territory.
 - g. 42 CFR § 423.505(m), which addresses the exchange and disclosure of certain Medicare Part D Prescription Drug Event (PDE) Data.
 - h. 42 CFR § 422.310(f), which addresses the allowable use and release of Medicare Advantage Encounter Data (referred to in regulation as “risk adjustment data”).
 - i. All other applicable laws and regulations, including those governing the confidentiality and disclosure, privacy, and data security of nonpublic information and data.
2. PMA:
- a. The HIPAA Privacy and Security Rules at 45 CFR parts 160 and 164.
 - b. Section 1935(c) of the Act, enacted in the Medicare Prescription Drug, Improvement and Modernization Act of 2003 (MMA) (P.L. 108-173, December 8, 2003) and implementing regulations. The MMA addresses the federal assumption of Medicaid prescription drug costs for Dually Eligible Individuals and the necessary, periodic data matches to identify and compute the number of full-benefit Dually Eligible Individuals for purposes of computing the phased-down state contributions. Regulations at 42 CFR § 423.910 established reporting by states and the frequency with which states must submit a data file (called the “MMA File” but sometimes referred to as the “State Phasedown File”) identifying Dually Eligible Individuals in their state (not applicable to territories).
 - c. All other applicable laws and regulations, including those governing the confidentiality and disclosure, privacy, and data security of nonpublic information and data.

C. Definitions

The following terms have the described meaning in this document:

1. “Accountable Care Organization (ACO) Assignment Data” means data that is being shared with states regarding Medicaid beneficiaries’ assignment to an ACO, including the ACO name and identification number (IDs) .
2. “Breach” is defined in OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017) (“OMB Memo M-17-12”), as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information, or (2) an authorized user accesses, or potentially accesses PII for an other than authorized purpose [HHS Policy and Plan for Preparing for the Responding to a Breach of Personally Identifiable Information (PII) (May 2020)].
3. “Care Coordination” means uses of the data (e.g., analysis, monitoring, or feedback) to support interventions, and/or the design of interventions, at the individual beneficiary level that have the potential to improve the care of Dually Eligible Individuals. Depending on circumstances, such intervention activities may include activities that qualify as “treatment” when performed by providers or may include certain activities listed in the first and second paragraphs of the definition of “Health Care Operations” in the HIPAA Privacy Rule at 45 CFR § 164.501.
4. “CMS” means the Centers for Medicare & Medicaid Services. CMS regulatory authority includes administration and oversight of the Medicare program, and oversight of the federal portion of the Medicaid program and State Children's Health Insurance Program, the Health Insurance Marketplace, and related quality assurance activities.
5. “CMS Data” means any of the data retrieved from the Privacy Act Systems of Records (SORs) cited in Section III.B, below, that are sent from CMS to the PMA under this Agreement and the corresponding DRA. CMS Data includes individually-identifiable derivative data and Specified Medicare Data as defined below.
6. “CMS DRA” or “DRA” means the executed “Medicaid-Medicare Dually Eligible Data Request and Attestation Form” that corresponds to this Agreement. The CMS DRA tracks the disclosure(s) of CMS Data to the PMA.
7. “CMS DRA Custodian Form” means the “Medicaid-Medicare Dually Eligible Data Request and Attestation Custodian Form.” The CMS DRA Custodian Form supplements the CMS DRA Form, and tracks Data Custodians that provide data storage for the PMA. By signing, the Data Custodians acknowledge the terms specified in the CMS DRA and CMS DRA Custodian Form.
8. “Data Custodian” means the individual or entity that is tasked by the PMA with primary responsibility for ensuring that the data received under this Agreement is used, maintained, and disclosed in accordance with the terms, conditions, safeguards and procedures set forth out in this Agreement and applicable law.

9. “Downstream User” means any person or entity (e.g., a treating practitioner, contractor, business associate, or subcontractor of the PMA – including a managed care plan) that receives CMS Data from the PMA in accordance with the terms of this Agreement and the corresponding DRA.
10. “Dually Eligible Individual” or “Dually Eligible Beneficiary” means an individual who is entitled to both Medicare benefits under Title XVIII of the Act and benefits provided by medical assistance programs under Title XIX of the Act.
11. “Enrollment Database File” or “EDB File” refers to the file produced from the EDB data query process between CMS and a state to determine eligibility and enrollment information for Dually Eligible Individuals. The EDB File includes detailed Medicare beneficiary information on Medicare Parts A and B only. The EDB File was retired effective June 30, 2022 but continues to be referenced here because EDB File data may still reside in state systems.
12. “Encounter Data” means the record submitted by a Medicare Advantage Organization (MAO) to CMS pursuant to 42 CFR § 422.310 about an enrollee receiving any item(s) or service(s) provided through Medicare and, where an MAO serves Dual Eligible Beneficiaries, through Medicaid), under a prepaid, capitated, or any other risk-based payment methodology. Encounter Data records are maintained in the CMS Encounter Data System (EDS).
13. “Health Care Operations” means those activities described in the first and second paragraph of the definition of that term in the HIPAA Privacy Rule at 45 CFR § 164.501, or the fraud and abuse-related activities described in § 164.506(c)(4).
14. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996.
15. “Incident” is defined by OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017), as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
16. “Medicaid” means the health benefit program established under Title XIX of the Act.
17. “Medicare” means the health benefit program established under Title XVIII of the Act.
18. “Medicare-Medicaid Coordination Office” or “MMCO” means the Federal Coordinated Health Care Office of CMS.
19. “MMA File” or “State Phasedown File” means the file a state submits to CMS to identify Dually Eligible Individuals in the state, including full-benefit and partial-benefit Dually Eligible Individuals (that is, those individuals who get Medicaid help with Medicare premiums, and, often, for cost-sharing). Its name derives from the

- legislation under which it was created, the MMA, and is described in section 1935 of the Act and at 42 CFR 423.910. It is inapplicable to territories.
20. “Medicare-Medicaid Data Sharing Program” means the elective process under which CMS shares Medicare data with PMAs for the purposes of Care Coordination, Program Integrity, and/or Quality Improvement. Under this process, CMS discloses Specified Medicare Data to the PMA.
 21. “Participating Medicaid Agency” or “PMA” means a state or territory Medicaid agency. PMA includes such parties’ contractors, subcontractors, and agents that work on behalf of such Medicaid agency to carry out Medicaid program functions.
 22. “PDE Data” means Medicare Part D Prescription Drug Event data that are reported to CMS by Part D prescription drug plan sponsors.
 23. “Personally Identifiable Information” or “PII” is defined in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)*, and refers to information which can be used to distinguish or trace an individual’s identity, either alone or when combined with information that is linked or linkable to a specific individual.
 24. “Program Integrity” refers to activities aimed at preventing, deterring, detecting, investigating, examining, prosecuting, litigating, defending against, correcting, or otherwise addressing health care fraud, waste, or abuse—including improper payments in the PMA’s Medicaid program. Depending on the circumstances, such activities may fall under the HIPAA Privacy Rule provisions regarding “health care fraud and abuse detection or compliance,” as described in the fourth paragraph of the HIPAA Privacy Rule’s definition of Health Care Operations and codified at 45 CFR § 164.506(c)(4), or “health oversight” as provided in 45 CFR § 164.512(d).
 25. “Protected Health Information” or “PHI” has the same meaning as provided in the definition of “Protected Health Information” in the HIPAA Privacy Rule at 45 CFR § 160.103.
 26. “Quality Improvement” means uses of the data (e.g., analysis, monitoring, or feedback) to support interventions, and/or the design of interventions, at the individual dual eligible beneficiary level that have the potential to improve or assess the quality of care of Dually Eligible Individuals or may include certain activities described in the first and second paragraphs of the definition of “Health Care Operations” in the HIPAA Privacy Rule at 45 CFR § 164.501.
 27. “Specified Medicare Data” means any of the following types of data that CMS shares as part of the Medicare-Medicaid Data Sharing Program for Care Coordination, Quality Improvement, or Program Integrity, including, but not limited to: Medicare Part A and Part B claims data, PDE data, Medicare eligibility and enrollment data, Minimum Data Set (MDS) data, Outcome and Assessment Information Set (OASIS) data, and Medicare Part C encounter data from EDS. Specified Medicare Data includes derivative files built by or for the PMA out of Specified Medicare Data that

is subject to this Agreement. Specified Medicare Data represents a specific subset of CMS Data.

28. "State Buy-in File" or "Buy-in File" means the data exchange between CMS and a state or territory where the state or territory sends CMS a data file to determine beneficiary Part A and B premiums liability.
29. "Territory & State Beneficiary Query" or "TBQ" means the data query where a PMA requests data from the CMS MDB to determine eligibility and enrollment information for Dually Eligible Individuals. Under this query process, PMAs query for detailed Medicare beneficiary information on Medicare Parts A, B, C (Medicare Advantage), and D (including plan enrollment and Low-Income Subsidy (LIS) eligibility).

II. RESPONSIBILITIES OF THE PARTIES

A. CMS Responsibilities

Following the execution of this Agreement and the corresponding CMS DRA, CMS will send CMS Data to the PMA in a timely and secure manner. The CMS Data may be sent electronically or physically, as determined by CMS.

CMS will maintain a record of all CMS Data that CMS provides to the PMA under this Agreement.

B. PMA Responsibilities

The PMA attests that it will maintain, use, and disclose the CMS Data in accordance with this Agreement, the corresponding DRA, and other applicable law, including any applicable state laws.

CMS Data obtained under this Agreement may be used and disclosed only for purposes specifically indicated in this Agreement or as required by law; other uses and disclosures are not permitted. However, the PMA may request to use or disclose the CMS Data for additional purposes outside of this Agreement; such requests are subject to CMS review and approval before such uses or disclosures may occur.

1. CMS Medicare-Medicaid Data Sharing Program, only:

In order to receive Specified Medicare Data under the Medicare-Medicaid Data Sharing Program, the PMA must submit a request to CMS that includes the following: (1) an acknowledgement that the PMA is a HIPAA-covered entity; (2) a list of the requested data files and, if applicable, data elements; and (3) an attestation that the Specified Medicare Data being requested is the "minimum necessary" to carry out the stated use of the data, as defined in the HIPAA Privacy Rule at 45 CFR § 164.502(b). CMS will only approve requests for Specified Medicare Data that assert that the PMA is requesting it for the PMA's Quality Improvement, Care Coordination, and/or Program Integrity purposes. In offering this CMS Data, CMS does not represent that the PMA has met all applicable HIPAA requirements for

requesting data under the applicable HIPAA requirements. The PMA should consult its own counsel to make those determinations prior to requesting this data from CMS. Furthermore, the PMA agrees that the PMA will only further disclose Encounter data upon CMS approval of clearly written data use justifications with identified downstream disclosure—such as to PMA contractors, vendors, or other business associates including Medicaid managed care plans—for each requested purpose.

The PMA must maintain a:

- a. list of all Downstream Users to whom the PMA provides CMS Data; and,
- b. data management plan that should be available upon CMS request.

III. DESCRIPTION OF THE DATA THAT MAY BE DISCLOSED

A. Exchanges and Data Files Covered by this Agreement

1. CMS Medicare-Medicaid Data Sharing Program – CMS shares (upon state request and CMS approval) Specified Medicare Data with state PMAs for the purposes of Care Coordination, Program Integrity, and/or Quality Improvement related to the state’s dually eligible population. If approved, CMS discloses (subject to the provisions of this Agreement, the corresponding DRA, and applicable federal law) Specified Medicare Data. The Medicare-Medicaid Data Sharing Program is elective.
2. Enrollment Database (EDB) File – The EDB process is a batch data query in which PMAs request data from CMS EDB to determine dual status eligibility. The EDB file was retired effective June 30, 2022, but EDB File data may still reside in state systems.
3. Territory & State Beneficiary Query (TBQ) File – The TBQ File is produced by a batch data query in which a PMA requests data from CMS’s Medicare Beneficiary Database (MBD) to determine dual status eligibility. The PMA submits a finder file, and CMS returns information on Medicare Parts A, B, C (Medicare Advantage), and D, including LIS eligibility. A PMA can submit TBQ Request Files to obtain batch data from the MBD (i.e., the data populated from the MMA file exchange). The TBQ File request process is elective.
4. The TBQ Application Programming Interface (API) is an alternative interface that PMAs can use to request the data included in the TBQ file and data on which of their state’s Medicaid beneficiaries are assigned to ACOs (“ACO Assignment Data”).
5. MMA File Exchange – State PMAs submit files at least monthly to the CMS MBD to identify all Dually Eligible Individuals in the state to CMS. CMS automatically returns a response file to the state upon processing the MMA File submission. The MMA File Exchange is associated with state Medicaid program operations and includes a state PMA and CMS only; there are no PMA downstream recipients.

6. State Buy-In File Exchange – CMS and PMAs exchange data on who is enrolled in Medicare and which parties are liable for paying that beneficiary’s Part A and B premiums. These data exchanges support state/territory, CMS, and the Social Security Administration (SSA) premium accounting, collections, and enrollment functions. To effectuate the state payment of Medicare Part A or Part B premiums, a state submits data on a buy-in file to CMS, which includes a record for each Medicare beneficiary for whom the state is adding or deleting coverage, or changing buy-in status. In response, CMS returns an updated transaction record, as well as a Part A or Part B billing record showing the state’s premium responsibility. The State Buy-in File Exchange is associated with state Medicaid program operations and includes either a state or territory PMA and CMS; or downstream users such as local agencies, contractors and managed care organizations.
7. ACO Operation System (ACO-OS) - CMS will provide PMAs data, sourced from ACO-OS, on which beneficiaries are assigned to ACOs via the TBQ Application Programming Interface (API) . .

B. Systems of Records

CMS will provide CMS Data from the following SORs:

1. CMS Encounter Data System (EDS), System No. 09-70-0506, published at 79 FR 34539 (June 17, 2014), as amended on February 14, 2018 (83 FR 6591). Data maintained in the EDS will be released pursuant to routine use number 2 and number 7, as set forth in the SORN.
2. Enrollment Data Base (EDB), System No. 09-70-0502; last modified at 73 FR 10249 (February 26, 2008), as amended on April 23, 2013 (78 FR 23938), February 18, 2016 (81 FR 8204) and February 14, 2018 (83 FR 6591). Data maintained in the EDB will be released pursuant to routine use number 2 and number 10, as set forth in the SORN.
3. Home Health Agency Outcome and Assessment Information Set (OASIS), System No. 09-70-0522, published at 72 FR 63906 (November 13, 2007), as amended on April 23, 2013 (78 FR 23938), May 29, 2013 (78 FR 32257) and February 14, 2018 (83 FR 6591). Data maintained in the OASIS will be released pursuant to routine use number 2 and number 8, as set forth in the SORN.
4. Long-term Care Minimum Data Set (MDS), System No. 09-70-0528, published at 72 FR 12801 (March 19, 2007), as amended on April 23, 2013 (78 FR 23938), May 29, 2013 (78 FR 32257) and February 14, 2018 (83 FR 6591). Data maintained in the MDS will be released pursuant to routine use number 2 and number 9, as set forth in the SORN.
5. Medicare Beneficiary Database (MBD), System No. 09-70-0536 last modified at 71 FR 70396 (February 14, 2018), as amended on April 23, 2013 (78 FR 23938), May 29, 2013 (78 FR 32257), February 14, 2018 (83 FR 6591). Data maintained in the

MBD will be released pursuant to routine use number 2 and number 11, as set forth in the SORN.

6. Third Party System (TPS), System No. 09-70-0505; published at 72 FR 36000 (July 2, 2007), as amended on February 14, 2018 (83 FR 6591). Data maintained in the TPS will be released pursuant to routine use number 2 and number 7, as set forth in the SORN.
7. Accountable Care Organization (ACO) Database System (ACO-OS), System No. 09-70-0598; published at 76 FR 58007 (September 19, 2011), as amended at [83 FR 6591](#) (February 14, 2018). Data maintained in the ACO-OS will be released pursuant to routine use number 4, as set forth in the SORN.
8. Chronic Condition Warehouse (CCW), System No. 09-70-0573, published at 79 FR 64802 (October 31, 2014), as amended on February 14, 2018 (83 FR 6591). Data maintained in the CCW will be released pursuant to routine use number 2 and number 11, as set forth in the SORN.
9. Medicare Integrated Data Repository (IDR), System No. 09-70-0571, published at 71 FR 74915 (December 13, 2006), as amended on October 20, 2011 (76 FR 65196), April 23, 2013 (78 FR 23938), May 29, 2013 (78 FR 32257) and February 14, 2018 (83 FR 6591). Data maintained in the IDR will be released pursuant to routine use number 2 and number 11, as set forth in the SORN.

C. Number of Records Involved and Operational Time Factors

As of 2023, the nationwide CMS Data records include over 13 million beneficiaries who are identified as Dually Eligible Individuals. Medicare records disclosed to the PMA under this Agreement will be limited to Dually Eligible Individuals residing in the PMA's state or territory.

The records exchanged under this Agreement and the corresponding DRA, specifically through the MMA File Exchange, will be used, in part, to confirm and/or add to CMS's current records regarding Dually Eligible Beneficiaries.

D. Data Elements Involved

The CMS Data made available in accordance with applicable federal law upon the request of the PMA and approval by CMS includes data elements for Dually Eligible Individuals residing in the PMA's state or territory to support activities as detailed in the Agreement. CMS Data made available under this agreement may include records that include some or all of the following data elements: beneficiary data (name, date of birth, sex, Social Security Number (SSN), mailing address, and Medicare Beneficiary Identifier (MBI)) and provider data (such as provider identification or certificate numbers). Data elements may vary depending on data file.

Under the MMA File Exchange and State Buy-in File Exchange, the PMA will provide the following data elements to CMS for purposes of identifying individuals for whom

data will be exchanged: name, date of birth, sex, and SSN.

Under the TBQ File data exchange, CMS does not retain the data from the PMA finder files.

Under the CMS Medicare-Medicaid Data Sharing Program data exchange, the PMA does not provide data to CMS.

IV. SECURITY PROCEDURES

A. By virtue of signing this agreement and the corresponding DRA, the PMA attests that the requested CMS Data will be protected as required by applicable law, including, but not limited to, the HIPAA Privacy and Security Rules at 45 CFR parts 160 and 164. This includes through the establishment of appropriate administrative technical and physical safeguards to protect the integrity, security, and confidentiality of the data, and preventing unauthorized use or access to it. Additionally, the PMA acknowledges that various federal laws (and, in many cases, state or territorial laws), including, but not limited to, the Privacy Act (5 U.S.C. § 552a), HIPAA, and Title 18 of the U.S. Code, as well as the corresponding regulations, specify administrative, civil, and/or criminal penalties to which individuals may be subject for conduct including, but not limited to, wrongful data access or acquisition, use, or disclosure. By virtue of signing this agreement, the PMA further attests that such safeguards will provide a level and scope of security that is not less than the level and scope of security requirements established for federal agencies by the OMB in:

1. [OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems,](#)
2. [Federal Information Processing Standard 200 entitled "Minimum Security Requirements for Federal Information and Information Systems,"](#) and
3. [Special Publication 800-53 "Recommended Security Controls for Federal Information Systems."](#)

The PMA acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually-identifiable or deducible information derived from the CMS Data is prohibited. Further, the PMA agrees that the CMS Data must not be physically moved, transmitted, or disclosed in any way from or by the Data Custodians' site(s) to an entity not listed in this Agreement or DRA without written approval from CMS, unless such movement, transmission, or disclosure is required by federal law. For example, CMS expects the PMA to, at minimum:

1. Protect PII and PHI that is furnished by CMS under this Agreement from loss, theft, or inadvertent disclosure;
2. Ensure that laptops and other electronic devices/media containing PII or PHI are encrypted and password-protected; and,

3. Send emails containing PII or PHI only if encrypted and being sent to and being received by e-mail addresses of persons authorized to receive such information.
- B. PMA agrees to restrict access to the CMS Data and any data created only to those users that have a need to know to perform their duties.
1. Administrative Safeguards: PMA will restrict access to the data exchange and to any data created by the exchange to only those users (e.g. employees, contractors, etc.) who need it to perform their official duties in connection with the uses of the data authorized in this Agreement. Further, PMA will advise all personnel who have access to the data exchanged and to any data created by the exchanged of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable Federal laws.
 2. Physical Safeguards: PMA will store the data exchanged and any data created by the exchange in an area that is physically and technologically secure from access by unauthorized persons at all times (e.g., door locks, card keys, biometric identifiers, etc.). Only authorized personnel will transport the data exchanged and any data created by the exchange. PMA will establish appropriate safeguards for such data, as determined by a risk-based assessment of the circumstances involved.
 3. Technical Safeguards: PMA will process the data exchanged, and any data created by the exchange, under the immediate supervision and control of authorized personnel in a manner that will protect the confidentiality of the data, so that unauthorized persons cannot retrieve any data by computer, remote terminal, or other means. Systems personnel must enter personal identification numbers when accessing data on the agencies' systems. PMA will strictly limit authorization to those electronic data areas necessary for the authorized user to perform their official duties.
 4. Application of Policy and Procedures: PMA will adopt policies and procedures to ensure that each agency uses the information contained in their respective records or obtained from each other solely as provided in this agreement. PMA and CMS will comply with these guidelines and any subsequent revisions.
- C. CMS reserves the right to conduct onsite inspections to monitor compliance with this Agreement and the corresponding DRA until such time CMS Data is destroyed and/or this Agreement and the corresponding CMS DRA is terminated.
- D. By virtue of signing this agreement and the corresponding DRA, the PMA attests that the requested data will be maintained, used, and disclosed only in a manner that is in accordance with the requirements of this agreement and the corresponding CMS DRA.

V. LOSS REPORTING

Incidents and/or Breaches that implicate PHI and/or PII must be addressed and reported, as applicable, in accordance with the HIPAA Breach Notification Rule, 45 CFR §§ 164.400 - 414.

The PMA shall further handle and report Incidents and Breaches in accordance with CMS' documented Incident Handling and Breach Notification procedures and in accordance with 42 CFR §§ 431.300 - 306. In addition to, and notwithstanding, PMA's compliance with all applicable obligations and procedures, PMA procedures must also address how the PMA will address the following, including reporting to CMS (including, but not limited to, MMCO):

- A. Identify Incidents and/or Breaches;
- B. Determine if PHI and/or PII, including MBI, is involved in Incidents;
- C. Determine whether the PHI and/or PII involved is related to CMS Data;
- D. Determine whether Breach Notification is required, and, if so, bear costs associated with the Breach Notification as well as any mitigation measures; and,
- E. Immediately notify CMS of any actual or suspected access to, or use or disclosure of, the data requested herein that is not in accordance with applicable law, including, but not limited to, the HIPAA Privacy or Security Rules. PMA further affirms that it will report any actual or suspected Incidents or Breaches of PHI and/or PII from the CMS data files, loss of these data, or disclosure to any unauthorized persons to the CMS Action Desk by telephone at (410) 786-2580 or by email notification at cms_it_service_desk@cms.hhs within one hour of discovery, and will cooperate fully with the federal security incident process.

If CMS determines that there may have been an Incident or Breach of the CMS Data or individually-identifiable derivative data or information by the PMA, its contractors and/or agents, and/or any Downstream Users that violates the terms of this Agreement, CMS may, in its sole discretion, immediately and unilaterally terminate this Agreement upon notice to PMA. PMA covenants and agrees to cease using and return and/or destroy all CMS Data therefrom in its possession, contractors'/agents' possession, or Downstream Users' possession immediately upon notice of termination for an Incident or Breach unless otherwise required by law. PMA agrees that it has the duty to protect and maintain the privacy and security of CMS Data, and that duty shall continue in full force and effect until such data are returned and/or destroyed. For any such data with respect to which return/destruction is not feasible, the privacy and security requirements of this Agreement and the corresponding DRA shall survive the termination or expiration of this Agreement.

VI. RECORDS USAGE AND REDISCLOSURE RESTRICTIONS

The PMA agrees that the CMS Data will be used and disclosed only as provided in this Agreement and the corresponding DRA.

VII. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The parties acknowledge that CMS retains all ownership rights to the CMS Data that PMA obtains under the terms of this Agreement, and that PMA does not obtain any right, title, or interest in any of the data furnished by CMS. The PMA will only retain the CMS Data for the

period of time required by law or for any processing or purpose related to the approved uses for which the data were received.

VIII. REIMBURSEMENT

No funds will be exchanged under this Agreement for any work to be performed by the PMA and CMS to carry out the requirements of this Agreement. CMS and PMA will provide data to each other at no cost.

IX. APPROVAL AND DURATION OF AGREEMENT

- A. **Effective Date:** This Agreement will become effective when signed by authorized officials of both parties.
- B. **Duration:** The duration of this Agreement is five years. Parties to this Agreement may execute a new agreement prior to the close of a five-year period. This Agreement remains in effect if both parties are working towards executing a new agreement.
- C. **Modification:** The parties may modify this Agreement at any time by a written modification agreed upon by both parties.
- D. **Termination:** Either party may unilaterally terminate this Agreement upon written notice to the other party, in which case the termination shall be effective 90 days after the date of that notice or at a later date specified in the notice. PMA agrees that it has the duty to protect and maintain the privacy and security of CMS Data, and that duty shall continue in full force and effect until such CMS Data is returned and/or destroyed. For any CMS Data or derivative data with respect to which destruction is not feasible, the privacy and security requirements of this Agreement and the corresponding DRA shall survive the termination or expiration of this Agreement.
- E. **Survival:** Terms and conditions in this Agreement for Security Procedures, Records Usage and Rediscovery Restrictions, and Retention and Disposition of Identifiable Records shall survive the termination or expiration of this Agreement until all data associated with this Agreement is returned or disposed of in accordance with the terms of this Agreement.

X. INTEGRATION CLAUSE

This Agreement constitutes the entire agreement of the parties with respect to its subject matter and supersedes all other agreements between the parties that pertain to the exchange of PHI and/or PII between the PMA and CMS, and, if applicable, the disclosure of Specified Medicare Data to the PMA for the purposes described in this agreement. PMA and CMS have made no representations, warranties, or promises outside of this agreement. This agreement takes precedence over any other documents that may be in conflict with it.

XI. PERSONS TO CONTACT

- A. CMS contacts are:

Central MMCO Data Sharing mailbox: MMCODataSharing@cms.hhs.gov

Program and Policy

Kimberly Spalding Bush, Director
 Program Alignment Group
 Federal Coordinated Health Care Office
 Centers for Medicare & Medicaid Services
 7500 Security Boulevard
 Location: S3-13-05
 Baltimore, MD 21244-1850
 Telephone: (410) 786-3232
 E-Mail: kimberly.spaldingbush@cms.hhs.gov

Nicole Perry, Health Insurance Specialist
 Program Alignment Group
 Federal Coordinated Health Care Office
 Centers for Medicare & Medicaid Services
 7500 Security Boulevard
 Baltimore, MD 21244-1850
 Telephone: 410-353-2563
 E-Mail: nicole.perry@cms.hhs.gov

Privacy and Agreement Issues

Barbara Demopulos, CMS Privacy Act Officer
 Division of Security, Privacy Policy and Governance
 Information Security and Privacy Group
 Office of Information Technology
 Centers for Medicare & Medicaid Services
 7500 Security Boulevard
 Location: N1-14-40
 Baltimore, MD 21244-1850
 Telephone: (443) 608-2200
 E-mail: Barbara.Demopulos@cms.hhs.gov

B. Participating Medicaid Agency contacts are:

(list all relevant PMA contacts)

[PMA POC Name]

[Position title of PMA POC]

[Name of PMA Office or Agency]

[PMA mailing street address]

[City, State, ZIP Code]

[Telephone: (xxx) xxx-xxxx]

[E-mail address for PMA POC]

XII. 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, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved by: (Signature of Authorized CMS Program Official)

**Steve Ludwig, Deputy Director
Program Alignment Group
Federal Coordinated Health Care Office
Centers for Medicare & Medicaid Services**

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, and confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

Approved By: (Signature of Authorized CMS Approving Official)

**Patrick Newbold
Chief Information Officer (CIO) &
Director, Office of Information Technology (OIT)
Centers for Medicare & Medicaid Services (CMS)**

Date:

C. Participating Medicaid Agency Approving Official

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

NAME OF PARTICIPATING MEDICAID AGENCY

State Name:

Medicaid Agency Name:

Approved By: (Signature of Authorized State or Territory Approving Official)

Name:

Date:

Title:

Affiliation: