COMPUTER MATCHING AGREEMENT BETWEEN
DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES
AND
STATE BASED ADMINISTERING ENTITIES
FOR
DETERMINING ELIGIBILITY FOR ENROLLMENT IN APPLICABLE STATE HEALTH SUBSIDY PROGRAMS UNDER THE PATIENT PROTECTION AND AFFORDABLE CARE ACT
Department of Health and Human Services No. 2504
Centers for Medicare & Medicaid Services No. 2025-11

Projected Effective Date: **October 1, 2025**
Projected Expiration Date: March 31, 2027

I. PURPOSE, LEGAL AUTHORITIES, AND DEFINITIONS

A. Purpose

The purpose of this Computer Matching Agreement (Agreement) is to establish the terms, conditions, safeguards, and procedures under which the Department Health and Human Services, Centers for Medicare & Medicaid Services (CMS) will disclose certain information (including information CMS receives from other federal agencies under related matching or query agreements) to the State Based Administering Entities (AE), to assist them in verifying applicant information, as required by the Patient Protection and Affordable Care Act of 2010 (PPACA), in order to make Eligibility Determinations for enrollment in "applicable State health subsidy programs," including exemption from the requirement to maintain Minimum Essential Coverage (MEC) or from the individual responsibility payment.

Information will be shared between CMS and AEs, and among AEs, for the purpose of making Eligibility Determinations, and for purposes of avoiding dual enrollment, particularly to verify whether applicants and enrollees on the Federally-facilitated Exchange (FFE) or State-based Exchanges (SBE) are currently eligible for or enrolled in a Medicaid/CHIP program. All information will be shared through the CMS Data Services Hub (Hub). Each party (CMS and each AE) is a Source Agency, and each AE is a non-Federal (recipient) agency under this agreement. The responsible component for CMS is the Center for Consumer Information & Insurance Oversight (CCIIO).

By entering into this Agreement, the Parties agree to comply with the terms and conditions set forth herein, as well as applicable laws and regulations. The terms and conditions of this Agreement will be carried out by authorized officers, employees, and contractors of CMS and the participating AE. For each State agency signatory to this Agreement, CMS and the relevant AE are each a "Party" and collectively "the Parties."

B. Legal Authorities

The following statutes govern or provide legal authority for the uses, including disclosures of data under this Agreement:

1. This Agreement is executed pursuant to the Privacy Act 5 United States Code (U.S.C.) § 552a and the regulations and guidance promulgated thereunder, including Office of Management and Budget (OMB) Circular A-108 "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act" published at 81 FR 94424 (Dec. 23, 2016), and OMB guidelines pertaining to computer matching published at 54 FR 25818 (June 19, 1989). The Privacy Act at 5 U.S.C. § 552a(b)(3) authorizes a Federal agency to disclose information about an individual that is maintained in a system of records, without the individual's prior written consent, when the disclosure is pursuant to a routine use published in a System of Records Notice (SORN) as required by 5 U.S.C. § 552a(e)(4)(D). CMS has published a routine use for its applicable system of records which authorizes the disclosures CMS makes to each AE under this Agreement.

2. This Agreement is executed to implement certain health care reform provisions of the Patient Protection and Affordable Care Act of 2010 (Public Law 111-148, 42 U.S.C. § 18001 et seq.), as amended by the Health Care and Education Reconciliation Act (Public Law 111-152) referred to collectively as the Patient Protection and Affordable Care Act (PPACA), and implementing regulations at 42 Code of Federal Regulations (CFR) Parts 431, 435, 457, and 45 CFR Parts 155-157.

3. Section 1331 of the PPACA authorizes States to establish Basic Health Plans (BHP), and BHP regulations require that states administering BHP verify whether an individual meets the eligibility requirements in § 1331(e) for enrollment in a BHP. BHP also require periodic redeterminations of eligibility and the opportunity to appeal denials of eligibility under 42 CFR § 600.335.

4. Medicaid and CHIP programs require periodic renewals and redeterminations of eligibility for those programs and the opportunity to appeal denials of eligibility under §§ 1902(a)(8) and 1902(a)(3) of the Social Security Act (the Act) and 42 CFR §§ 435.916, 457.343 and Part 431, Subpart E and Part 457 Subpart K. Pursuant to 42 CFR § 435.945 and 42 CFR § 457.348, a Medicaid or CHIP agency must disclose certain income and eligibility information, subject to regulations at 42 CFR part 431, subpart F, needed for verifying eligibility for an Insurance Affordability Program.

5. 26 U.S.C. § 6103(1)(21) authorizes the disclosure of certain tax return information as defined under 26 U.S.C. § 6103(b)(2) (hereinafter "Federal Tax Information," abbreviated "FTI") for purposes of determining eligibility for certain Insurance Affordability Programs and prohibits disclosure of Federal tax information to an Exchange or State agency administering a State program, unless the program is in compliance with the safeguards requirements of 26 U.S.C. § 6103(p)(4), and unless the information is used to establish eligibility for certain Insurance Affordability Programs.

C. Definitions

For purposes of this Agreement, the following definitions apply:

1. "Administering Entity" or "AE" means a state-based entity administering an Insurance Affordability Program. An AE may be a Medicaid agency, a Children's Health Insurance Program (CHIP), a basic health program (BHP), or a State Based Exchange (SBE) established under § 1311 of the PPACA.

2. "Applicant" means an individual who is seeking eligibility for him or herself through an application submitted to an Exchange, excluding those individuals seeking eligibility for an exemption from the individual shared responsibility payment pursuant to subpart G of Title 45, or transmitted to the Exchange by an agency administering an insurance affordability program for at least one of the following: Enrollment in a QHP through the Exchange; or Medicaid, CHIP, and the BHP, if applicable.

3. "Applicant Filer" means an Applicant, an adult who is in the Applicant's household, as defined in 42 CFR § 435.603(f), or family, as defined by CFR 1.36B-1(d), an Authorized Representative of the Applicant, or if the Applicant is a minor or incapacitated, someone acting responsibly for the Applicant, excluding those individuals seeking eligibility for an exemption.

4. "APTC" means advance payments of the premium tax credit specified in § 36B of the Internal Revenue Code (IRC) (as added by § 1401 of the PPACA) which are provided on an advance basis on behalf of an eligible individuals enrolled in a QHP through an Exchange in accordance with §§ 1402 and 1412 of the PPACA.

5. "Authorized Representative" means an individual or organization who acts on behalf of an Applicant or beneficiary and meets the requirements set forth for Exchanges at 45 CFR § 155.227 or for Medicaid at 42 CFR § 435.923.

6. "Breach" is defined in OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, (January 3, 2017) as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

7. "CHIP" means the Children's Health Insurance Program established under Title XXI of the Act.

8. "CSR" means cost-sharing reductions for an eligible individual enrolled in a silver

level plan through the Exchange or for an individual who is an Alaskan Native/American Indian enrolled in a QHP through the Exchange.

9. “Eligibility determination” means the determination of eligibility for enrollment in an applicable State health subsidy program, or certifications of exemption from the requirement to maintain MEC or the individual shared responsibility payment. The term “eligibility determination” includes initial assessments and determinations, mid-year and annual redeterminations, and renewals, and any appeal process related to an eligibility determination.

10. "Enrollee" means an individual enrolled in a QHP through an Exchange or in enrolled in a BHP.

11. "Exchange" means a Federally-facilitated Exchange or a State-based Exchange (including a not-for-profit exchange) established under sections 1311(b), 1311(d)(1), or 1321(c)(1) of PPACA.

12. "Hub" or "CMS Data Services Hub" is the CMS managed, single data exchange for AEs to interface with Federal agency partners. Hub services allow for adherence to Federal and industry standards for security, data transport, and data safeguards as well as CMS policy for AEs for eligibility determination and enrollment services.

13. “Insurance Affordability Programs” means (1) the program under title I of the PPACA that makes available coverage in a QHP through an Exchange with APTC or CSR; (2) a Medicaid program under title XIX of the Act; (3) a Children’s Health Insurance Program (CHIP) under title XXI of the Act; and (4) a program under § 1331 of the ACA establishing qualified basic health plans.

14. “Medicaid” means the health insurance program established under Title XIX of the Act and is one of the Insurance Affordability Programs.

15. “Non-Federal Agency” is defined in the Privacy Act at 5 U.S.C. § 552a(a)(10) and means any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program.

16. "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 means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

17. "PPACA" means Patient Protection and Affordable Care Act of 2010 (Public Law No. 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law No. 111-152) (collectively, the PPACA).

18. “Qualified Health Plan” or “QHP” means an insurance plan under the PPACA that is certified by an Exchange in each state in which it is sold, provides essential health

benefits, follows established limits on cost-sharing (like deductibles, copayments, and out-of-pocket maximum amounts), and satisfies other requirements.

19. "Recipient Agency" is defined in the Privacy Act at 5 U.S.C. § 552a(a)(9) and means any federal agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program.

20. "Relevant Individual" means any individual listed by name and SSN on the application whose PII or financial information may bear upon an eligibility determination of an Applicant for enrollment in a QHP and/or for an Insurance Affordability Program or certificate of exemption.

21. "Security Incident" means "Incident," which is defined in 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.

22. "State-based Exchange," or "SBE," means an Exchange established and operated by a State and approved by HHS under 45 CFR § 155.105.

23. "Source Agency" is defined in the Privacy Act at 5 U.S.C. § 552a(a)(11) and means any federal agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program.

II. RESPONSIBILITIES OF THE PARTIES

A. CMS Responsibilities:

1. CMS will develop and maintain the Hub to support activities described in this Agreement.

2. CMS will develop the appropriate form and manner of submission of data to and from the Hub.

3. CMS will develop procedures and conditions through and under which an AE may request information via the Hub from available data sources, which include but are not limited to CMS, the Internal Revenue Service (IRS), Social Security Administration (SSA), Department of Homeland Security (DHS), Department of Veterans Affairs (VA), Department of Defense (DOD), Peace Corps (PC), Office of Personnel Management (OPM), and commercial databases or income and employment, to support eligibility determinations.

4. CMS will develop procedures through which an AE can request information via the Hub to support identity proofing for an Applicant or Application Filer prior to the release of matching data under this Agreement.

5. CMS will not use the Hub to transmit data to an authorized AE to support an eligibility determination, unless specifically authorized in Section IV of this Agreement.

6. CMS will provide Congress and the OMB with advance notice of this matching program and, upon completion of their advanced review, will publish the required matching notice in the Federal Register.

B. AE Responsibilities:

1. AE will only request data or data verifications from CMS that are necessary to make eligibility determinations as described under Section IV.C.

2. AE will develop procedures to transmit Applicant, Enrollee, or Relevant Individual information to CMS in order to verify or validate data and attestations made on the application for eligibility determinations, or to meet other program requirements as specifically authorized in Section IV of this Agreement.

3. AE will provide the data elements identified in Section IV.C. of this Agreement in the manner established by the Secretary of HHS when transmitting Applicant, Enrollee, or Relevant Individual information to the Hub.

4. AE will not use or re-disclose matching data received from the Hub to any entity or individual for any purpose other than making eligibility determinations. Nothing in this Agreement shall be construed to prohibit disclosure where required by applicable law. Notwithstanding, AE may not use or disclose Federal Tax Information to any entity or individual unless such disclosure is permitted under the IRC and approved by the IRS.

5. Where AE is a Medicaid or CHIP agency in a state where the FFE is operating, it will respond to requests sent via the Hub to verify an Applicant's or Enrollee's enrollment in the Medicaid or CHIP program.

6. AE will comply with identity proofing procedures described in "Guidance Regarding Identity Proofing for the Exchange, Medicaid, and CHIP, and the Disclosure of Certain Data Obtained through the Hub" issued to the AE by CMS.

III. JUSTIFICATION AND ANTICIPATED RESULTS

A. Cost-Benefit Analysis

In accordance with 5 U.S.C. § 552a(u)(4)(A), a cost benefit analysis (CBA) is included as Attachment 1. The CBA covers this and seven other "Marketplace" matching or query programs which CMS conducts with other federal agencies and the AEs. The CBA demonstrates that monetary costs to operate all eight Marketplace matching or query

programs exceed $74.5 million per year but does not quantify direct governmental monetary benefits sufficient to offset the costs, because the Marketplace matching or query programs are not intended to avoid or recover improper payments. The CBA, therefore, does not demonstrate that this matching program is likely to be cost-effective.

However, other supporting justifications and mitigating factors support approval of this CMA, as described below. OMB guidance provides that the Privacy Act "does not require the showing of a favorable ratio for the match to be continued. The intention is to provide Congress with information to help evaluate the cost-effectiveness of statutory matching requirements with a view to revising or eliminating them where appropriate." See OMB Guidelines, 54 FR 25818 at 25828.

B. Other Supporting Justifications

Even though the Marketplace matching or query programs are not demonstrated to be cost-effective, ample justification exists in the CBA sections III (Benefits) and IV (Other Benefits and Mitigating Factors) to justify DIB approval of the matching programs, including the following:

1. The Marketplace matching or query programs have resulted in efficient and accurate consumer eligibility determinations and MEC checks and substantially reduce the administrative burden on CMS and AEs.
2. The matching or query programs provide a significant benefit to the public by allowing CMS and AEs to quickly and accurately determine consumer eligibility for QHPS and IAPs while minimizing consumer burden.
3. An efficient eligibility and enrollment process contributes to greater numbers of consumers enrolling in Marketplace QHPs, resulting in a reduction of the uninsured population, therefore improving overall health care delivery.
4. Continuing to use the current matching program structure, which is less costly than any alternative structure, is expected to increase the public's trust in the participating agencies as stewards of taxpayer dollars.

C. Specific Estimate of Any Savings

There are no cost savings to conducting the Marketplace matching or query programs, as opposed to not conducting them. By requiring a single, streamlined application process, the PPACA effectively required use of computer matching to make eligibility determinations. Therefore, the optimal cost-savings result is attained by limiting the costs of conducting the matches to the extent possible, and by using a matching program operational and technological process that is more efficient than any alternative process. CMS estimates that the cost of operating the matches is about $74.5 million per year. CMS' analysis suggests that the benefits of increased enrollment outweigh the costs given the increase in private insurance coverage through the PPACA.

IV. RECORDS DESCRIPTION

The Privacy Act, at 5 U.S.C. § 552a(o)(1)(C), requires that each CMA specify a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program.

A. System of Records

The CMS System of Records that supports this matching program is the "CMS Health Insurance Exchanges System (HIX)", CMS System No. 09-70-0560, last published in full at 78 FR 63211 (October 23, 2013) and amended at 83 FR 6591 (February 14, 2018). Routine use 3 authorizes CMS' disclosures of identifying information about Applicants to source agencies to obtain match responses, and routine use 2 authorizes CMS' disclosures of match responses to AEs for use in this matching program.

B. Number of Records Involved

The Congressional Budget Office (CBO) previously estimated that up to 12 million beneficiary records in total may be transacted for coverage in QHP and other Insurance Affordability Programs. For 2020, the CBO estimated that 10 million individuals would sign up for QHP coverage through the marketplaces (including SBEs), one million for BHP coverage, and 70 million for Medicaid/CHIP coverage.

C. Specified Data Elements Used in the Match

1. From AE to CMS. The AE will send data identifying Applicants, Enrollees, and Relevant Individuals, via the Hub, as part of the request for data or verification of attestations on an application for eligibility for enrollment in a QHP through an Exchange, for another Insurance Affordability Program, or for a certification of exemption. The data elements the AE may submit via the Hub may include the following:

    a. Social Security Number (if applicable)
    b. Last Name
    c. First Name
    d. Date of Birth

From CMS to AE. CMS will receive via the Hub the data inputs listed above, transmit them via the Hub to the appropriate Federal agency or other approved data source, receive responses from the data source, and transmit those responses through the Hub to the requesting AE. Alternatively, CMS will receive via the Hub the data inputs listed above and provide a response based on data received in a secure electronic manner from the appropriate Federal agency, with such response being transmitted through the Hub to the requesting AE. The data elements the AE will receive from CMS via the Hub may include:

a. Validation of SSN

b. Verification of Citizenship or Immigration Status
c. Incarceration status
d. Eligibility and/or enrollment in certain types of MEC
e. Income, based on Federal Tax Information (FTI), Title II benefits, and current income sources
f. Quarters of Coverage
g. Death Indicator

2. Exact data elements sent to CMS and returned by CMS will vary by query and AE. These data outputs, and the manner of transfer required by the Secretary of HHS, are specified in CMS Federal Data Services Hub Business Service Definitions (BSD) guidance, organized by information technology (IT) business service. The following IT business services have been identified for the purposes outlined in this Agreement and AEs must comply with the associated BSD requirements when using the following IT business services:

a. SSA Composite (includes SSN validation, citizenship status, indication of death, incarceration, Title II benefits, and quarters of coverage).

i. This service is available to all AEs.

b. Verify Lawful Presence (which includes verification of immigration status and naturalized or derived citizenship status).
i. This service is available to all AEs.

c. Verify Annual Income and Family Size (Federal Tax Information).
i. This service is available to all AEs authorized to receive Federal Tax Information from the IRS.

d. Verify Current Income from other sources.
i. This service is available to all AEs.

e. Verify Employer-Sponsored Insurance (ESI) MEC.
i. This service is available to all SBEs and BHPs.

f. Verify Non-ESI MEC.
i. Medicaid/CHIP can use this service to verify Medicaid MEC.
ii. SBEs and BHPs can use this service to verify Medicare, TRICARE, VHA, and Peace Corps MEC.

g. Periodic Eligibility Verification Bulk Service (includes date of death and Medicare MEC).
i. This service will be available to all AEs, but is specifically designed for use by SBEs for periodic checks of current enrollees.

h. Redetermination & Renewal Verification Bulk Service (includes IRS income, IRS Failure to Reconcile (FTR) indicators, SSA Title II benefit income, Equifax current income, and Medicare MEC).

i. This service is available to all AEs. IRS income and FTR indicators are available only for AEs authorized to receive Federal Tax Information from the IRS.

D. Projected Starting and Completion Dates of the Matching

Effective Date – Approximately October 1, 2025
Expiration Date – March 31, 2027 (March 31, 2028, if renewed for one year)

V. NOTICE PROCEDURES

The Privacy Act, at 5 U.S.C. § 552a(o)(1)(D), requires that each matching agreement specify procedures for providing individualized notice at the time of application and periodically thereafter.

A. CMS will publish notice of the matching program in the Federal Register, as required by the Privacy Act at 5 U.S.C. § 552a(e)(12).

B. At the time of application, AE will provide individual notice (Privacy Act Statement) on the approved streamlined eligibility application regarding the collection, use, and disclosure of the Applicant's PII by the AE; such application shall be either the CMS developed model application (approved under OMB No. 0938-1191) or an alternate state application approved by HHS. The single streamlined application which CMS has developed includes a Privacy Act statement (available at https://www.healthcare.gov/privacy/ and https://www.cms.gov/marketplace/applications-and-forms/individual-short-form-instructions.pdf) describing the purposes for which the information is intended to be used and the authority which authorizes the collection of the information. The Privacy Act statement also links to a more fulsome explanation of how the Applicant's PII may be used (available at https://www.healthcare.gov/how-we-use-your-data/) In addition, when an Applicant submits an application for an exemption, depending on whether the SBE will make the eligibility determination for the exemption itself or whether the SBE will utilize the Federally managed service to make the eligibility determination for an exemption, the SBE or CMS will provide individual notice on the exemption application regarding the collection, use and disclosure of the Applicant's PII. The exemption application contains a Privacy Act statement describing the purposes for which the information is intended to be used and the authority which authorizes the collection of the information.

At the time of redetermination, SBE must provide redetermination notices that will inform individuals about how their information is used, and where more information can be found about privacy and security policies. Requirements for Medicaid and CHIP agencies to provide notice at the time of Medicaid and/or CHIP renewal are at 42 CFR §§ 435.916 and 457.343.

VI. VERIFICATION PROCEDURES AND OPPORTUNITY TO CONTEST FINDINGS

As required by the Privacy Act, at 5 U.S.C. § 552a(p), each matching agreement must specify procedures for verifying information produced in the matching program and an opportunity to contest findings.

A. Verification and Opportunity to Contest Findings

Correcting information with a relevant data source is not necessary to resolve an inconsistency or complete an eligibility determination. Resolving an inconsistency with an AE will not correct information contained in the records of the relevant data source.

Information that is provided via the Hub by other data sources, and information that originates with other data sources and is disclosed by CMS through the Hub, cannot be corrected by contacting CMS. Individuals must contact the relevant data source that provided those records via the Hub in order to correct such records. An individual seeking to contest the content of information that HHS or another data source provided to an Exchange for matching purposes should contact the relevant data source. Under 26 U.S.C. § 7852(e), FTI cannot be corrected without filing an amended tax return with the IRS.

B. Contesting Findings

In the event that information attested to by an individual for matching purposes is inconsistent with information received through electronic verifications obtained by the AE through the Hub, the AE must provide notice to the individual that the information the individual provided did not match information received through electronic verifications as follows:

1. If the AE is an Exchange, an individual seeking to resolve inconsistencies between attestations and the results of electronic verification for the purposes of completing an eligibility determination should be provided the opportunity to follow the procedures outlined in 45 CFR § 155.315(f). The AE will provide the individual with the proper contact information and instructions for resolving the inconsistency.

2. If the AE is an agency administering a Medicaid or CHIP program, an individual seeking to resolve an inconsistency between an attestation and the result of an electronic verification for the purposes of completing an eligibility determination should be provided the opportunity to follow the procedures outlined in 42 CFR §§ 435.952, 435.956 and 457.380. The AE will provide the individual with the proper contact information and instructions for resolving the inconsistency.

3. Per 42 CFR § 600.345, if the AE is a BHP, it must elect either Exchange verification procedures at 45 CFR §§ 155.315 and 155.320, or Medicaid verification procedures at 45 CFR § 435.945-956; and must resolve inconsistencies as set forth in paragraphs VI.B.1 and 2 above.

VII. DISPOSITION OF MATCHED ITEMS

The AE and CMS will retain the electronic files received from the other Party only for the period of time required for any processing related to the matching program and will then destroy all such data by electronic purging, unless the AE or CMS is required to retain the information for enrollment, billing, payment, program audit purposes, or for legal evidentiary purposes or where otherwise required by law to retain the information. In case of such retention, the AE and CMS will retire the retained data in their databases in accordance with the applicable Federal Records Retention Schedule (44 U.S.C. § 3303a). The AE and CMS will not create permanent files or separate systems comprised solely of the data provided by the other agency.

VIII. SECURITY PROCEDURES

A. Safeguards

The Parties shall comply with all applicable regulations regarding the privacy and security of PII (see, e.g., § 1411(g) of the PPACA, 45 CFR § 155.260). Medicaid and CHIP agencies shall comply with all applicable regulations regarding the privacy and security of PII, including provisions of the HIPAA Privacy and Security Rules at 45 CFR Parts 160 and 164, that govern protections for individually identifiable health information (such as eligibility for health care under the Medicaid or CHIP program(s)).

B. The Parties must comply with the latest version of the suite of documents entitled, "Minimum Acceptable Risk Standards for Exchanges" (MARS-E) as published by CMS, which prov security standards with which the Parties must comply. Further, the Parties agree to comply with all current guidance (including revisions to MARS-E as they are published and made effective), regulations, and laws that apply to them on this subject.

C. Officers, employees and agents who inspect or disclose FTI obtained pursuant to this Agreement in a manner or for a purpose not so authorized by 26 U.S.C. 6103 are subject to the criminal sanction provisions of 26 U.S.C. sections 7213 and 7213A, and 18 U.S.C. section 1030(a)(2), as may be applicable. In addition, the AE could be required to defend a civil damages action under section 7431.

D. An AE shall ensure that its employees, contractors, and agents implement the appropriate administrative, physical and technical safeguards to protect matching data furnished by CMS under this Agreement (including matching data which constitutes PII) from loss, theft or inadvertent disclosure.

1. Administrative Safeguards: Both Parties will advise all users who will have access to the matching data (including but not limited to matched and to any data derived from the match) of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in applicable Federal laws.

2. Physical Security/Storage: Both Parties will store the matching data and any data derived from the match in an area that is physically and technologically secure from access by unauthorized persons during duty hours, as well as non-duty hours or when not in use (e.g., door locks, card keys, biometric identifiers, etc.). Only authorized personnel will transport the matching data and any data derived from the match. Both Parties will establish appropriate safeguards for such data, as determined by a risk- based assessment of the circumstances involved.

3. Technical Safeguards: Both Parties agree that the data exchanged under this Agreement will be processed under the immediate supervision and control of authorized personnel to protect the confidentiality of the data in such a way that unauthorized persons cannot retrieve any such data by means of computer, remote terminal, or other means. AE personnel must enter personal identification numbers when accessing data on the Party's systems. Both Parties will strictly limit authorization to those electronic data areas necessary for authorized persons to perform his or her official duties.

4. An AE shall ensure that its employees, contractors, and agents understand that they are responsible for safeguarding this information at all times, regardless of whether or not the AE employee, contractor, or agent is at his or her regular duty station.

5. An AE shall ensure that its employees', contractors', and agents' laptops and other electronic devices/media containing matching data that constitutes PII are encrypted and/or password protected.

6. An AE shall ensure that its employees, contractors, and agents send e-mails containing matching data that constitutes PII only if encrypted and being sent to and received by e- mail addresses of persons authorized to receive such information. In the case of FTI, AE employees, contractors, and agents must comply with IRS Publication 1075's rules and restrictions on e-mailing FTI.

7. An AE shall ensure that its employees, contractors, and agents restrict access to the matching data to only those authorized AE employees, contractors, and agents who need such data to perform their official duties in connection with purposes identified in this Agreement; such restrictions shall include, at a minimum, role- based access that limits access to those individuals who need it to perform their official duties in connection with the uses of data authorized in this Agreement ("authorized users"). Further, the AE shall advise all users who will have access to the data provided under this Agreement and to any data derived from the data matching contemplated by this Agreement 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. The AE shall require its contractors, agents, and all employees of such contractors or agents with authorized access to the data disclosed under this Agreement, to comply with the terms and conditions set forth in this Agreement, and not to duplicate, disseminate, or disclose such data unless authorized under this Agreement.

8. For receipt of FTI, AE agree to maintain all FTI sourced from the IRS in accordance with IRC section 6103(p)(4) and comply with the safeguards requirements set forth in Publication 1075, "Tax Information Security Guidelines for Federal, State and Local Agencies", which is the IRS published guidance for security guidelines and other safeguards for protecting FTI pursuant to 26 CFR 301.6103(p)(4)-1. In addition, IRS safeguarding requirements require all AE to which CMS provides FTI to:

    a. Establish a central point of control for all requests for and receipt of FTI and maintain a log to account for all subsequent disseminations and products made with/from that information, and movement of the information until destroyed, in accordance with Publication 1075, section 3.0.

    b. Establish procedures for secure storage of FTI consistently maintaining two barriers of protection to prevent unauthorized access to the information, including when in transit, in accordance with Publication 1075, section 4.0.

    c. Consistently label FTI obtained under this Agreement to make it clearly-identifiable and to prevent access by unauthorized individuals. Any duplication or transcription of FTI creates new records which must also be properly accounted for and safeguarded. FTI should not be commingled with other Agency records unless the entire file is safeguarded in the same manner as required for FTI and the FTI within is clearly labeled in accordance with Publication 1075, section 5.0.

    d. Restrict access to FTI solely to officers, employees, agents, and contractors of AE whose duties require access for the purposes of carrying out this Agreement. Prior to access, AE must evaluate which personnel require such access on a need-to-know basis. Authorized individuals may only access FTI to the extent necessary to perform services related to this Agreement, in accordance with Publication 1075, section 5.0.

    e. Prior to initial access to FTI and annually thereafter, ensure that AE employees, officers agents, and contractors that will have access to FTI receive awareness training regarding the confidentiality restrictions applicable to the FTI and certify acknowledgement in writing that they are informed of the criminal penalties and civil liability provided by §§ 7213, 7213A, and 7431 of the IRC for any willful disclosure or inspection of FTI that is not authorized by the Code, in accordance with Publication 1075, section 6.0.

    f. Prior to initial receipt of FTI, have an IRS approved Safeguard Security Report (SSR). Each AE's Head of Agency must certify the SSR fully describes the procedures established for ensuring the confidentiality of FTI, addresses all outstanding actions identified by the Office of

Safeguards from a prior year's SSR submission; accurately and completely reflects the current physical and logical environment for the receipt, storage, processing and transmission of FTI; accurately reflects the security controls in place to protect the FTI in accordance with Publication 1075 and the commitment to assist the Office of Safeguards in the joint effort of protecting the confidentiality of FTI; report all data incidents involving FTI to the Office of Safeguards by e-mail at SafeguardReports@cms.hhs.gov within 24 hours of discovery, and to cooperate with the Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident; support the Office of Safeguards' on-site review to assess compliance with Publication 1075 requirements by means of manual and automated compliance and vulnerability assessment testing, including coordination with information technology (IT) divisions to secure pre-approval, if needed, for automated system scanning and to support timely mitigation of identified risk to FTI in a Corrective Action Plan (CAP) for as long as FTI is received or retained. SSR will be transmitted in electronic format and on the template provided by Office of Safeguards using an IRS approved encryption method in accordance with Publication 1075, Section 7.0.

g. Ensure that FTI is properly destroyed or returned to the IRS when no longer needed based on established AE record retention schedules in accordance with Publication 1075, section 8.0, or after such longer time required by applicable law.

h. Conduct periodic internal inspections of facilities where FTI is maintained to ensure IRS safeguarding requirements are met and will permit the IRS access to such facilities as needed to review the extent to which AE is complying with the requirements of this section.

i. Ensure information systems processing FTI are compliant with § 3544(a)(1)(A)(ii) of the Federal Information Security Management Act of 2002 (FISMA). Each AE will maintain an SSR which fully describes the systems and security controls established at the moderate impact level in accordance with National Institute of Standards and Technology (NIST) standards and guidance. Required security controls for systems that receive, process, store and transmit Federal tax returns and FTI are provided in Publication 1075, section 9.0.

j. Report suspected unauthorized inspection or disclosure of FTI within 24 hours of discovery to the appropriate Agent-in-Charge and to the IRS Office of Safeguards in accordance with IRS Publication 1075.

k. Allow IRS to conduct periodic safeguard reviews of the AE to assess whether security and confidentiality of FTI is maintained consistent with the safeguarding protocols described in Publication 1075. Periodic safeguard reviews will involve the inspection of AE facilities and

contractor facilities where FTI is maintained; the testing of technical controls for computer systems storing, processing, or transmitting FTI; review of AE recordkeeping and policies and interviews of AE employees and contractor employees as needed, to verify the use of FTI and assess the adequacy of procedures established to protect FTI.

l. Recognize and treat all IRS Safeguards documents and related communications as IRS official agency records; that they are property of the IRS; that IRS records are subject to disclosure restrictions under Federal law and IRS rules and regulations and may not be released publicly under state Sunshine or Information Sharing/ Open Records provisions and that any requestor seeking access to IRS records should be referred to the Federal Freedom of Information Act (FOIA) statute. If the AE determines that it is appropriate to share Safeguards documents and related communications with another governmental function/branch for the purposes of operational accountability or to further facilitate protection of FTI that the recipient governmental function/branch must be made aware, in unambiguous terms, that Safeguards documents and related communications are property of the IRS; that they constitute IRS official agency records; that any request for the release of IRS records is subject to disclosure restrictions under Federal law and IRS rules and regulations, and that any requestor seeking access to IRS records should be referred to the Federal Freedom of Information Act (FOIA) statute. Federal agencies in receipt of FOIA requests for safeguards documents must forward them to IRS for reply.

E. Incident Handling and Reporting

l. Each AE is responsible for creating its own formal written policies and procedures for responding to privacy and security incidents in accordance with applicable state and Federal law, MARS-E, and CMS guidance. Each AE shall handle and report Incidents in accordance with its organization's documented incident handling and breach notification procedures. These policies and procedures should have the adequate scope, definitions and assignments of roles and responsibilities, and explanations to enable the AE to:

a. Identify incidents involved matching data that constitute PII.

b. Report all suspected or confirmed incidents involving matching data that constitute PII. This requirement applies to all system environments. Identify and convene a core response group within the AE who will determine the risk level of incidents involving matching data that constitute PII and determine risk-based responses to such incidents.

c. Determine whether breach notification is required, and, if so, identify appropriate breach notification methods, timing, source, and contents from among different options, and bear costs associated with the notice as well as any mitigation.

d. Limit the disclosure of information about individuals whose information may have been compromised, misused, or changed without proper authorization, and the persons who improperly disclosed matching data that constitute PII, to authorized Federal, state, or local law enforcement investigators in connection with efforts to investigate and mitigate the consequences of any such incidents.

2. AE shall report all suspected or confirmed incidents (including loss of suspected loss of involving matching data that constitute PII) within one hour of discovery to CMS, and to IRS if the incident involves FTI, as follows:

a. SBEs and BHPs shall report a suspected or confirmed Security or Privacy Incident or Breach of PII within one (1) hour using the CMS ACA Security and Privacy Incident Response Template to the CMS CMS_IT_Service_Desk@cms.hhs.gov, or via phone at 1-800-562-1963. That will inform the appropriate designated CMS staff and notify the affected Federal agency data sources: (e.g., Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management, and Veterans Health Administration). Similarly, if an SBE suspects a security or privacy incident may warrant a disconnection of the system-to-system connection to CMS and/or the Hub due to the severity of the incident and potential threat to CMS and other Federal systems, the SBE must immediately contact the CMS IT Service Desk via e-mail at CMS_IT_Service_Desk@cms.hhs.gov or via phone at 1-800-562-1963.

b. SBEs and BHPs report any incident involving FTI to the IRS Office of Safeguards by e-mail to SafeguardReports@cms.hhs.gov. SBE should not wait until after their own internal investigation has been conducted to report an incident to CMS and the IRS.
Medicaid and CHIP agencies operating in a state in which the FFE operates shall report a suspected or confirmed Security or Privacy Incident or Breach of PII within one (1) hour using the CMS ACA Security and Privacy Incident Response Template to the CMS_IT_Service_Desk@cms.hhs.gov, or via phone at 1-800-562-1963. That will then inform the appropriate designated CMS staff and the affected Federal agency data sources (i.e., Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management, and Veterans Health Administration). State Medicaid and CHIP agencies are also responsible for reporting any suspected or confirmed incident involving FTI directly to the office of the appropriate Special Agent-in-Charge and the IRS Office of Safeguards by e-mail at SafeguardReports@irs.gov within 24 hours of discovery of any potential breach, loss, or misuse of FTI. Incident reporting procedures are contained in § 1.8.4 of the IRS Publication 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf).

c. A Medicaid and/or a CHIP agency, when operating as an AE performing Exchange functions under an SBE shall report a suspected or confirmed Security or Privacy Incident or Breach of PII within one (1) hour using the CMS ACA Security and Privacy Incident Response Template to the CMS_IT_Service_Desk@cms.hhs.gov, or via phone at 1-800-562-1963. That will inform the appropriate CMS staff and the affected Federal agency data sources (i.e., Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management, or Veterans Health Administration). The Medicaid/CHIP agency shall contact the office of the appropriate Special Agent-in-Charge and the IRS Office of Safeguards by e-mail at SafeguardReports@irs.gov within 24 hours of discovery of any potential breach, loss, or misuse of FTI. Incident reporting procedures are contained in § 1.8.4 of the IRS Publication 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf). The Medicaid and/or CHIP agency shall handle and report incidents in accordance with the organization's documented incident handling and breach notification procedures in accordance with 42 CFR §§ 431.300-431.306, and 435.945.

3. AE shall refer to the Interconnection Security Agreement (ISA) for instructions on handling disconnects from the Hub. The Change Management section provides instructions for handing an emergency or planned disconnect, initiated by the AE or CMS, as well as restoration procedures.

F. Administering Entity Opt-Out for Receiving FTI

Notwithstanding the requirements related to FTI in this Section VIII or in any section of this Agreement, if an AE that is a Party to this Agreement opts out of receiving FTI provided by the IRS in connection with eligibility determinations and does not receive such FTI, that AE shall not be bound by any of this Agreement's terms governing the receipt, use, disclosure or safeguarding of FTI. Should that AE revise its position at any time during the term of this Agreement and so notify CMS of its intent to receive FTI, the AE must comply with the terms of this Agreement as it relates to the safeguarding of FTI as of the date of such notice; provided, however, that no FTI will be disclosed to the AE without an IRS approved Safeguard Security Report.

IX. RECORDS USAGE, DUPLICATION, AND REDISCLOSURE RESTRICTIONS

A. CMS and AE will only use, duplicate, and disclose the electronic files and data provided by the other Party under this Agreement as permitted or required by this Agreement or as required by applicable Federal law.

B. CMS and AE will not use the matching data to extract information concerning individuals therein for any purpose not specified by this Agreement or allowed by applicable SORN or Federal law.

C. The matching data exchanged under this Agreement remains the property of the Party that provided the data and will be retained and destroyed as described in Section VII of this matching Agreement.

D. CMS and AE will restrict access to data solely to officers, employees, and contractors of CMS and AE.

1. The AE will restrict access to the matching data to Applicants, Enrollees, Application Filers, and Authorized Representatives of such persons. AE shall execute with each individual or entity such as agents or brokers that (a) gain access from the AE to PII submitted to an Exchange or (b) collect, use, or disclose PII gathered directly from Applicants, or Enrollees while that individual or entity is performing the functions outlined in its agreement with the AE, a written contract or agreement that includes (i) a provision describing the functions to be performed by the individual or entity and strictly limiting the use and disclosure of PII to those functions; (ii) a provision(s) binding the individual or entity to comply with the same privacy and security standards and obligations that are made applicable to the PII under this Agreement, as appropriate, and specifically listing or incorporating those privacy and security standards and obligations; (iii) a provision requiring the individual or entity to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls; (iv) a provision requiring the individual or entity to inform the AE of any change in its administrative, technical, or operational environments defined as material within the contract; (v) a provision that requires the individual or entity to bind any downstream entities to the same privacy and security standards and obligations to which the individual or entity has agreed in its contract or agreement with the AE.

   Each Medicaid and Children's Health Insurance Program (CHIP) agency also must assure that it will provide safeguards which restrict the use or disclosure of information concerning Applicants and recipients to purposes directly connected with the administration of the Medicaid and CHIP programs. This includes the disclosure of electronic data used to make an Eligibility Determination. 42 CFR § 431, subpart F, including §§ 431.301, 431.302, 431.303, 431.305, 435.945, and 42 CFR § 457.1110.

2. Any individual who receives information from an Exchange or via the Hub in connection with an eligibility determination for enrollment in an applicable State health subsidy program and who knowingly and willfully uses or discloses information obtained pursuant to this Agreement in a manner or for a purpose not authorized by 45 CFR § 155.260 and § 1411(g) of the PPACA is potentially subject to the civil penalty provisions of Section 1411(h)(2) of the PPACA and 45 CFR § 155.285, which carries a fine of up to $25,000.

X. RECORDS ACCURACY ASSESSMENTS

CMS currently estimates that 99% of the information within the Enrollment System's Administrative Data Repository (ADR) is accurate for PPACA purposes in cases where: (1) an exact applicant match is returned, and (2) the applicant has an enrollment status of "verified," and (3) the applicant's enrollment period coincides with the start/end dates received from the Hub.

XI. COMPTROLLER GENERAL ACCESS

Pursuant to 5 U.S.C. § 552(o)(l)(K), the Government Accountability Office (Comptroller General) may have access to all CMS and AE records, as necessary, in order to verify compliance with this Agreement.

XII. REIMBURSEMENT/FUNDING

This Agreement does not itself authorize the expenditure or reimbursement of any funds. Nothing in this Agreement obligates the Parties to expend appropriations or enter into any contract or other obligations.

XIII. DURATION OF AGREEMENT

A. Effective Date and Duration

The Effective Date of this Agreement will be approximately October 1, 2025, provided that CMS first reported the proposal to re-establish this matching agreement to the Congressional committees of jurisdiction and OMB in accordance with 5 U.S.C. § 552a(o)(2)(A) and (r) and OMB Circular A-108 and, upon completion of their advance review, CMS published notice of the matching program in the Federal Register for at least thirty days in accordance with 5 U.S.C. 552a(e)(12).

The initial term of this Agreement will be eighteen (18) months.

The AE and CMS may, within three (3) months prior to the expiration of this Agreement, renew this Agreement for not more than one additional year if CMS and AE certify the following to the HHS DIB:

1. The matching program will be conducted without change; and
2. CMS and AE have conducted the matching program in compliance with this Agreement.

B. Termination

This Agreement may be terminated at any time upon the mutual written consent of the Parties. Either party may unilaterally terminate this Agreement upon written notice to the other party, in which case the termination will be effective ninety (90) days after the date of the notice, or at a later date specified in the notice provided this date does not exceed the approved duration for the agreement. A copy of this notification should be submitted to the Secretary, HHS DIB.

XIV. LIABILITY

A. Each party to this Agreement shall be liable for acts and omissions of its own employees.

B. Neither Party shall be liable for any injury to another Party's personnel or damage to another Party's property, unless such injury or damage is compensable under the Federal Tort Claims Act (28 U.S.C. § 346(b)), or pursuant to other Federal statutory authority.

C. Neither party shall be responsible for any financial loss incurred by the other, whether directly or indirectly, through the use of any data furnished pursuant to this Agreement.

D. Nothing in this Agreement is intended, or should be construed, to create any right or benefit, substantive procedural, enforceable at law by any third party against the United States, its agencies, officers or employees, or either Party.

E. Nothing in this Agreement shall be construed as a waiver of sovereign immunity against suits by third persons.

XV. INTEGRATION CLAUSE

This Agreement constitutes the entire agreement of the Parties with respect to its subject matter and supersedes all other data exchange agreements between the Parties that pertain to the disclosure of data between AE and CMS for the purposes described in this Agreement. CMS and AE 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.

XVI. PERSONS TO CONTACT

A. The CMS contacts are:

1. **Programmatic Issues between CMS and the Federal Hub Data Partners**
   Terence Kane
   Director
   Division of Eligibility Verifications
   Marketplace Eligibility and Enrollment Group
   Center for Consumer Information and Insurance Oversight
   Centers for Medicare & Medicaid Services
   7501 Wisconsin Avenue
   Bethesda, MD 20814
   Telephone: (301) 492-4449
   Fax: (443) 821- 4263
   Email: Terence.Kane@cms.hhs.gov

2. **State Based Exchange Programmatic Issues**

Jenny Chen Director
Director of State Technical Assistance
State Marketplace and Insurance Programs Group
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services
7501 Wisconsin Avenue
Bethesda, MD 20814
Telephone: 301-492-5156
E-mail: Jenny.Chen@cms.hhs.gov

Robert Yates
Deputy Director
Division of State & Grant Operations
State Marketplace and Insurance Programs Group
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Bethesda, MD 20814
Telephone: 301-492-5151
E-mail: Robert.Yates@cms.hhs.gov

3. **Medicaid/CHIP Programmatic Issues**

Sarah DeLone
Acting Director
Children & Adults Health Programs Group Center
for Medicaid and CHIP Services Centers for
Medicaid & Medicare Services Baltimore, MD
21244-1850
Telephone: (410) 786-0615
E-Mail: Sarah.Delone2@cms.hhs.gov

4. **Medicaid/CHIP System Issues**

Brent Weaver
Director
Data and Systems Group
Center for Medicaid and CHIP Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Mail Stop: S2-22-27
Location: C2-02-11
Baltimore, MD 21244-1850
Telephone: (410)786-0070
Fax: (443)796-5622
E-mail: Brent.Weaver@cms.hhs.gov

5. **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
Baltimore, MD 21224-1849
Telephone: (443) 608-2200
Mail Stop: N1-14-40
E-mail: Barbara.Dempoulos@cms.hhs.gov

6. **Marketplace Privacy and Security Issues**
Kathryn Wetherby
Acting Director
Marketplace Information Technology Group
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, MD 21224-1850
Telephone: (410)786-0198
E-mail: Kathryn.Wetherby@cms.hhs.gov

B. The contact person for the AE can be found on the Administering Entity's signature page.

XVII. CENTERS FOR MEDICARE & MEDICAID SERVICES SIGNATURES

Source Agency Certification:

The authorized 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 the organization to the terms of this Agreement.

Electronic Signature Acknowledgement: The signatories may sign this document electronically by using an approved electronic signature process. Each signatory who electronically signs this renewal agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

As the authorized representative of the recipient agency named above, I certify that: (1) the subject matching program has been conducted in compliance with the existing computer matching agreement between the parties; and (2) the subject matching program will continue without any change for one additional year upon approval of this renewal by the Data Integrity Board of each party.

A. Centers for Medicare & Medicaid Services Program Official and Approving Appointed Senior Level Official

PETER J. NELSON -S Digitally signed by PETER J. NELSON -S
Date: 2025.08.20 21:57:10 -04'00'

Peter Nelson
Director
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services

Date: 8/20/2025

B. Center for Medicaid and CHIP Services Program Official

The authorized 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 the organization to the terms of this Agreement.

SARA M. VITOLO -S Digitally signed by SARA M. VITOLO -S
Date: 2025.08.27 14:25:52 -04'00'

Sara Vitolo
Deputy Director
Center for Medicaid and CHIP Services
Centers for Medicare & Medicaid Services

Date:_____

C. Centers for Medicare & Medicaid Services Approving Official

As the authorized representative of the source agency named above, I certify that: (1) the subject matching program has been conducted in compliance with the existing computer matching agreement between the parties; and (2) the subject matching program will continue without any change for one additional year upon approval of this renewal by the HHS Data Integrity Board.

Leslie Nettles -S Digitally signed by Leslie Nettles -S
Date: 2025.08.12 16:57:30 -04'00'

Leslie Nettles
Director
Division of Security, Privacy and Oversight, and
Senior Official for Privacy
Information Security and Privacy Group
Office of Information Technology
Centers for Medicare & Medicaid Services

Date: 8/12/25

D. U.S. Department of Health and Human Services Data Integrity Board Official

As Chair of the Data Integrity Board of the source agency named above, based on the signed Source Agency Certification and the signed Recipient Agency Certification, I approve renewal of this matching program for one additional year.

Clark Minor
Clark Minor (Sep 22, 2025 15:21:15 EDT)

Clark Minor
Chairperson
HHS Data Integrity Board
U.S. Department of Health and Human Services

Date:

E. Participating AE Program Official

1. AE Model

The AE will request via the Hub information necessary to verify applicant information in support of an eligibility determination. The Hub will facilitate the sharing of information for a data match with Federal agencies and other data sources, as appropriate for the type of eligibility determination and AE, and then transmit the results of the data match back to the AE.

The AE under this Agreement is:

- ☐ Medicaid Agency (Includes any Medicaid Agency Administering Eligibility Verifications for a State-based Exchange)
- ☐ Children's Health Insurance Program
- ☐ Basic Health Program
- ☐ State-based Exchange

The AE will verify applicant information for the following eligibility determinations:

- ☐ Medicaid
- ☐ Children's Health Insurance Program
- ☐ Basic Health Program
- ☐ Qualified Health Plan Enrollment
- ☐ Advance Payments of the Premium Tax Credit
- ☐ Cost-Sharing Reductions

The authorized program official, who should be designated by the AE, and 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. Each AE will sign a separate copy of this Agreement.

Approved by (Signature of Authorized AE Official)

_____

Name

Title

Organization

Date:_____

Attachment 1: Master Cost-Benefit Analysis

EXCHANGE COMPUTER MATCHING PROGRAMS: COST-BENEFIT ANALYSIS

Prepared by:
Center of Consumer Information and Insurance Oversight (CCIIO)
Centers for Medicare and Medicaid Services (CMS)

COST-BENEFIT ANALYSIS FOR EXCHANGE MATCHING PROGRAMS

Updated JULY 2, 2025

Table of Contents

Introduction

This cost benefit analysis (CBA) provides information about the costs and benefits of conducting the eight required Exchange[1] matching or query programs, which are conducted under matching or other agreements between CMS and each federal data source agency and between CMS and state administering entities (AEs). The objective of the matches is to support the enrollment of eligible individuals in appropriate health coverage programs.

The matches enable AEs to make efficient and accurate eligibility determinations and redeterminations for enrollment in qualified health plans (QHPs), insurance affordability programs, Medicaid and Children Health Insurance Programs (CHIP), and Basic Health Programs (BHP), and support the issuance of certificates of exemption to individuals who are exempt from the individual mandate to maintain health insurance coverage. The matches provide for a single streamlined application process as required by the Affordable Care Act (ACA), support accurate and real-time eligibility determinations, and ensure that consumers can enroll in the correct program or be properly determined to be exempt from needing coverage.

The matches enable AEs to verify individuals' attested application responses with matched data elements from relevant federal data sources based on the type of eligibility determination being performed. These data elements may include verification of citizenship or immigration status (Department of Homeland Security), household income (Internal Revenue Service), social security information (Social Security Administration), and access to non-employer-sponsored and/or employer-sponsored minimum essential coverage (MEC). Non-employer-sponsored coverage includes coverage through TRICARE (Department of Defense), Veteran's Health Benefits (Department of Veterans Affairs, Veterans Health Administration), Medicaid, Medicare, or benefits through service in the Peace Corps. Employer-sponsored coverage for Federal Employee Health Benefits can be verified with the Office of Personnel Management (OPM).

While the matches support accurate eligibility determinations, which help avoid improper payments (e.g., improper payments of tax credits to ineligible individuals), no data is available to quantify the amount of improper payments avoided. In addition, the match results are not currently used to identify or recover past improper payments. Consequently, there are no estimates of avoided or recovered improper payments in key elements 3 and 4 (i.e., the

[1] 'Exchange' means a State-based Exchange (SBE, including a not-for-profit Exchange) or a Federally-Facilitated Exchange (FFE) established under sections 1311(b), 1311(d)(1), or 1321(c)(1) of the PPACA. For purposes of this analysis, all references to an Exchange shall refer equally to and include a state agency that is responsible for administering the Insurance Affordability Program under which individuals and small businesses may enroll in Qualified Health Plans (QHP) in the state.

"benefits" portion) of the CBA to offset against the personnel and computer costs estimated in key elements 1 and 2 (i.e., the "cost" portion) of the CBA, so the four key elements of the CBA do not demonstrate that the matching or query programs are likely to be cost-effective. However, the CBA describes other justifications (i.e., factors demonstrating that the matches are effective in maximizing enrollments in QHPs and are structured to avoid unnecessary costs) which support Data Integrity Board (DIB) approval of the matching programs. As permitted by the Privacy Act at 5 U.S.C. § 552a(u)(4)(B), the Justification section of each matching agreement requests the DIB(s) to determine, in writing, that the CBA is not required in this case to support approval of the agreement and to approve the agreement based on the other stated justifications.

The four key elements and sub-elements required to be addressed in the CBA are summarized on the CBA template below. The name of each key element and sub-element is highlighted in bold in the narrative portion of the CBA to indicate where that element is discussed in more detail.

A. Costs

Costs for the recipient and source agencies are primarily personnel costs associated with maintenance and operations supported by information technology resources; therefore, key elements 1 and 2 (personnel costs and computer costs) are combined in this analysis. Note that more detail on the summary figures that follow is provided in later sections of this document.

For Agencies –

- **CMS (Recipient Agency):** $47.9 million ($2.3 million internal costs; $45.6 million external costs) per year.
- **Source Federal Agencies:** $26.6 million per year (reimbursed by CMS)
- **State AEs:** No data developed.
- **Justice Agencies:** Not applicable, as these matching programs are not currently used to detect and recover past improper payments and therefore do not generate collection cases for justice agencies to investigate and prosecute.

For Clients (Applicants/Consumers), and any Third Parties assisting them –

- Opportunity costs (time required to apply for coverage) are quantified as $1.2 billion per year ($49.52 per application x 24.3 million consumers enrolled in QHPs).

For the General Public –

- No data developed. Costs to the public (such as discouragement of legitimate potential participants from applying, and threats to privacy, Constitutional rights, and other legal rights) would be less significant in these matching programs than in other matching programs, because these matching programs are intended to support enrollments and are not currently used to detect and recover past improper payments.

B. Benefits

Avoidance of Future Improper Payments

For advance payments of the premium tax credit (APTC), consumers must reconcile the tax credit at the time of tax filing, and so improper payment is mitigated. For state and federal costs associated with Medicaid coverage, the avoidance of future improper payment is not quantified here. However, the use of matching programs mitigates the risk of fraud and abuse by applicants or third parties by requiring that personal information provided on an eligibility application match known data on the individuals.

Recovery of Improper Payments and Debts

Not applicable, because data from the Exchange matching programs are not currently used to identify and recover improper payments and debts.

C. Matching Program Structure

The Patient Protection and Affordable Care Act, Public Law No. 111-148, as amended by the Health Care and Education Reconciliation Act of 2010, Public Law No. 111-152 (ACA) requires that each state develop secure electronic interfaces for the exchange of data under a matching program using a single application form for determining eligibility for all state health subsidy programs.

CMS has entered into matching agreements with the following federal source agencies: 1) Social Security Administration (SSA), 2) Department of Homeland Security (DHS), 3) Internal Revenue Service (IRS), 4) Department of Veterans Affairs (VA) Veterans Health Administration (VHA), 5) Department of Defense (DoD), 6) Office of Personnel Management (OPM), and 7) the Peace Corps. In addition, CMS has developed a matching program that is executed with every state AE, including state Medicaid and CHIP agencies and State-based Exchanges (SBEs). CMS designed the Federal Data Services Hub (the "Hub") to be a centralized platform for the secure electronic interface that connects all AEs and trusted data sources (TDS).

Without the Hub, each State AE would be required to enter into a separate arrangement with each federal agency to determine whether applicants for state health subsidy programs are eligible for coverage. If the match operations were conducted through separate arrangements outside of the Hub, the costs to CMS, the source federal agencies, the AEs, and consumers (applicants) would be significantly greater than under the current structure.

D. Background assumptions

CMS has made the following assumptions in developing this CBA:

- The ACA does not expressly mandate the use of computer matching, but effectively requires it by requiring a single, streamlined application process for consumers. Because matching must be conducted to provide the single, streamlined application process Congress required (i.e., is not optional), this CBA does not evaluate whether the matching programs should be conducted versus not conducted, but rather it evaluates whether the matching programs are efficiently structured and conducted, and whether the current structure is less costly than an alternative structure.
- Eight matching programs are currently operational. CMS receives data from seven source federal agencies (IRS, DHS, SSA, OPM, Peace Corps, VHA, and DoD) under separate respective individual CMAs. Under an eighth CMA, CMS makes the data from those seven source federal agencies, as well as CMS data regarding Medicare enrollment, available to state AEs; in addition, the eighth CMA makes state Medicaid and CHIP enrollment data available to CMS. The seven source federal agencies, CMS, and the state AEs are collectively known as the TDSs. All data from the TDSs are accessed by CMS and by state AEs via the Hub platform, rather than via direct access from any AE to any TDS.
- Any alternative, non-Hub structure that could be used instead of the current Hub structure would require many more than eight CMAs, as well as many more system interconnections and data transmissions between agencies.
- For a subset of the TDSs, CMS incurs a cost as the recipient agency. The cost of each data transaction is estimated based on a prior year's matching program budget and the estimated number of data transactions occurring that year.
- In addition to the TDSs themselves, additional entities are necessary to provide support services to the Hub. CMS therefore incurs external costs in the hiring, maintenance, and associated costs of contractors to perform numerous functions related to the Hub. In addition, costs are incurred for identity proofing of applicants, troubleshooting, procedure writing, and maintenance support.
- CMS has internal costs related to the funding of CMS federal staff and associated resources to complete processes and responsibilities related to the Hub and the matching programs.
- The benefit of these matching programs is to consumers who apply for and obtain health coverage. The private benefit to them is improved health care delivery and the expected value of the coverage (whether through private insurance, Medicaid, CHIP, or a Basic Health Plan, if applicable).
- Regarding the Recovery of Improper Payments and Debts (Key Element 4), CMS is not currently utilizing the data match result from the matching programs for payment and debt reconciliations; however, the benefit of the match does provide the potential to implement this capability in the future.

I. Costs

Costs for the recipient and source agencies are primarily personnel costs associated with maintenance and operations supported by information technology resources; therefore, **key elements 1 and 2 (personnel costs and computer costs) are combined in this analysis.**

A. Internal CMS Costs - $2.3 million / year

Most costs paid by CMS to implement the Exchange matching programs and the Hub are external costs paid to contractors, which are addressed in the next section. CMS' internal costs for federal staff tasked to work on these programs are approximately $2.3 million per year. The below chart attributes all of the costs to federal staff working in the Center for Consumer Information and Insurance Oversight (CCIIO) office; however, many teams across CMS provide support to the implementation of these programs, and CCIIO staff often have other programs in their portfolios beyond the Exchange matching programs and the Hub.

CCIIO Team	Estimated Annual Cost
Eligibility and Enrollment (E&E)	$844,053
SMIPG (State Policy)	$361,737
Marketplace Information Technology (MITG/HUB)	$1,085,211
Total	$2,291,001

B. External CMS costs: Hub operations - $45.6 million/ year

- ### Federal Data Services Hub (Hub) – $29 million / year

  The Hub is maintained by a CMS contract. While the initial build costs of the Hub were largely incurred before the implementation of the Exchange programs in 2013, there are ongoing costs associated with system maintenance, changes necessitated by ongoing technology development and new program implementation, and general system health monitoring. In fiscal year (FY) 2025, the average annual cost of the Hub contract was $29 million. The Hub supports many other Exchange program efforts besides the matching programs, including the transmission of data to and from insurance issuers, and electronic file transfer for many programs within the Exchange; as a result, $29 million is an overestimate of the annual Hub costs associated with Exchange matching program operations.

- ### Exchange Security Operations Center (SOC)

  The Exchange SOC is responsible for the security operations and maintenance for the Hub and the Federally-facilitated Exchange (FFE). For FY2025, the CMS Office of Information Technology (OIT) Information Security and Privacy Group (ISPG) budget team determined that there are no direct CCIIO budget contributions for the SOC

operation costs. Previously, ISPG took on security operations functions for the Exchange, and multiple funding sources were added to the OIT budget to share the cost load across funding sources. As there are no direct CCIIO contribution to the SOC budget, there were enterprise funding changes made to support the Exchange as part of the enterprise security program upon its inception.

- ### Exchange Operations Center (XOC) - $6.0 million / year

  The Exchange Operations Center (XOC) is an entity managed under the Exchange System Integrator contract tasked with coordinating the technical operations of the Hub and of the FFE. The XOC supports system availability, communication of system issues to stakeholders, and incident triage. Because the XOC budget line is not formally delineated for the Hub and for the FFE, the operational cost cited above is an overestimate of the costs specific to supporting Hub operations. The $6,012,506 cost estimate provided here covers both XOC operations as well as site reliability engineer and metrics costs in support of the XOC.

- ### Identity-Proofing Service Costs – $10.6 million / year

  Before consumer information can be submitted to a data source for data verification, a consumer's online account must be identity proofed. Remote identity proofing (RIDP) is a service supported through the Hub for AE programs. While identify proofing is not an eligibility requirement, it is a requirement for online application submission.

C. Costs paid by CMS to TDS agencies – $26.6 million / year

- ### Social Security Administration (SSA) - $3.5 million / year

  The SSA is the source of numerous data elements for the Hub: verification of the applicant's name, date of birth, citizenship, Social Security Number (SSN), a binary indicator for incarceration, Title II income (retirement and disability), and work quarters. Verification of an individual's SSN is a required precursor to accessing consumer information through the other Exchange matching programs.

  Matching with SSA data is accomplished through a reimbursable agreement with CMS. The total cost of the SSA contract with CMS in FY 2025 was $3,476,719.03 under Inter Agency Agreement (IAA) number IA25-34.

- ### Department of Homeland Security (DHS) – $22.5 million / year

  DHS is the verification source for naturalized and derived citizenship, and immigration status. The total cost of the DHS contract with CMS in FY 2025 was $22,500,000 under IAA number IA25-31.

  The DHS charges according to a graduated fee schedule for using the database called

"SAVE" (Systematic Alien Verification for Entitlements Program). There are up to 3 steps of SAVE verification process: Step 1 is a real-time "ping" to their system. Consumers who could not be successfully verified may go to Step 2, which takes 3-5 days for additional database searches. The third step requires manual touch from a DHS Status Verification Officer. Costs are currently $2.25 per use at Steps 1, 2 and 3. Ongoing automation through DHS's paperless initiative will impact these costs in the future.

- ### Veterans Health Administration (VHA) - $596K / year

  Data from the VHA are used to identify current enrollment in health coverage through the VHA, which is an eligibility factor for APTC and cost sharing reduction (CSR) programs. The VHA contract with CMS is transactions-based. The total cost of the VHA contract with CMS in FY 2025 was $595,902 under IAA number IA25-38.

- ### Office of Personnel Management - $25,100 / year

  For FY 2022, OPM charged CMS a flat fee of $25,100 under IAA number IA25-39.

- ### Other Trusted Data Sources

  CMS does not pay the other Trusted Data Sources (IRS, DoD, Peace Corps, and State Medicaid and CHIP Agencies) for access to and use of their data.

D. Consumer opportunity costs – non-monetary, but quantified

Applying for coverage does not have a monetary cost to applicants, but does have an opportunity cost. CMS estimates that the average time for a consumer to apply for and enroll (or re-enroll) in a QHP each year averages 1 hour and 12 minutes.[2] At a rate of $41.27 per hour, this opportunity cost is estimated at $49.52 per application per year. The complete number of applications submitted each year across all AEs is not known, but the total number of QHP enrollees for PY 2025 is 24.3 million,[3] resulting in a consumer opportunity cost of approximately $1.2 billion. It should be noted that this estimate does not include opportunity costs for enrollees in Medicaid, CHIP, or BHP, if applicable, programs, or for consumers who apply but do not subsequently enroll in coverage.

[2] Estimate is based on a 12 minute average to complete an application for QHP coverage plus an additional 1 hour for the consumer to provide supporting documentation to the Exchange should a data matching issue occur.

[3] Enrollees in QHPs have the opportunity each year to be automatically reenrolled in a QHP or to return to the Exchange to choose a new plan – however, Exchanges encourage enrollees to update their information and reevaluate their health coverage needs for the coming year. Furthermore, enrollees are required to report certain life changes as they occur, since they may impact coverage and/or participation in insurance affordability programs. CMS has elected to use the entire universe of 2025 QHP enrollees (24.3 million) in this CBA in order to present the most conservative case for consumer opportunity costs.

II. Benefits

A. Benefits to Agencies – not quantified

The Exchange matching programs improve the accuracy of data used for making program eligibility determinations and ensure that individuals are correctly determined and are not inappropriately enrolled in multiple programs. Improved data quality helps ensure that eligibility determinations and other decisions affecting APTC are accurate, which helps avoid future improper payments. This avoidance of future improper payments fits the third cost benefit analysis key element but hasn't been quantified.

Using data made available through the Exchange matching programs in combination with an individual applicant's attestation of his or her personal information is more reliable than relying solely on applicant attestations. The use of data matching mitigates the risk of fraud and abuse by applicants or third parties by requiring that personal information provided on an eligibility application match known data on the individuals.

B. Benefits to Enrollees of obtaining health coverage – quantified, but outside the scope of the 4 key elements

For PY2025, 24,319,713 consumers enrolled in a QHP across all Exchanges. Of these, 92% received APTC, with an average value of $550 per month (annualized to $6,600 per year). In total, therefore, approximately $148 billion in APTC will be provided to enrollees in Plan Year 2025.[4]

Approximately 51% of the QHP enrollees in PY2025 received financial assistance through cost-sharing reductions when enrolling in a silver-level plan. The financial estimate of this benefit is not quantified here, as it is dependent on individual utilization of medical services.
Additionally, a significant number of consumers receive health coverage through Medicaid, CHIP, or a BHP, if applicable, and received eligibility determinations for that coverage based on data made available through these agreements. Because of the wide variety in state approaches to making and reporting eligibility determinations, the number of enrollees in these programs is not quantified here.

The financial benefit of having health coverage, whether through a QHP, Medicaid, CHIP, or BHP, if applicable varies by individual and individual health needs, and is therefore not estimated here.
While these benefits to consumers are made possible in part by the Exchange matching

[4] 5/12/2025: Plan Year 2025 data from https://www.cms.gov/files/document/health-insurance-exchanges-2025-open-enrollment-report.pdf

programs, the benefits are ultimately paid with federal funds (or, in the case of Medicaid and CHIP enrollees, with a combination of federal and state funds). Neither that funding nor these benefits to consumers can be considered a direct cost or benefit of conducting the Exchange matching programs. As a result, these benefits are not directly applicable to this analysis.

C. Recovery of improper payments – not germane (not an objective) at this time

The fourth cost benefit analysis key element (recovery of improper payments and debts) is not germane to this cost benefit analysis, because data from the Exchange matching programs are not currently used to identify and recover improper payments and debts. Annual reconciliation and recovery of improper tax payments are performed by the IRS through a process that is independent of the Exchange matching programs and other CMS eligibility determination activities. While the Exchange matching programs could provide for annual and monthly reporting of data by Exchanges to the IRS and consumers for the purpose of supporting IRS's annual reconciliation, annual and monthly reporting is not currently an activity covered in the IRS-CMS CMA; rather, that information is exchanged between the agencies through Information Exchange Agreements. At most, the data used in the Exchange matching programs has the future potential benefit of being used in an analytical form, to assist IRS in identifying and/or recovering improper payments and debts.

Consideration of Alternative Approaches to the Matching Programs

In requiring a single, streamlined application process and specifying electronic data access, the ACA effectively required use of computer matching to make eligibility determinations. As a result, wholly manual alternatives for verification of application information (such as a paper-based documentation process) are not considered as a viable alternative in this analysis.

The Exchange matching programs currently leverage the Hub to minimize connections between AEs and the federal partners. This model has successfully met program needs by providing for a single, streamlined application process for consumers, and supporting accurate eligibility determinations, which in turn increase program integrity for the Exchange programs.

An alternative, non-Hub approach, for AEs to manage matching programs individually without using the Hub, was considered through this analysis. Without the Hub, each State AE would be required to enter into separate matching arrangements with each federal partner and build direct connections to each system. CMS believes a non-Hub approach would involve:

- More agreements to prepare and administer (there would be one agreement per AE with each TDS, in place of one agreement per AE with CMS, and one agreement per TDS with CMS);
- More TDS data transmissions to effect and secure (there would be one TDS transmission per AE, in place of each single TDS transmission to the Hub);
- More systems to maintain and secure, to store the TDS data (there would be one system per AE, in place of the single, central Hub system); and
- More copies of TDS data to correct when errors are identified (there would be one copy to correct in each AE system, instead of the single copy in the Hub system).

Based on this analysis, CMS believes the current structure minimizes duplication of effort and is therefore less costly for CMS, federal partners, and State AEs, than an alternative structure that would not leverage the Hub.

Conclusion

The Exchange matching programs are effectively required, not discretionary, in order to provide the single streamlined application process Congress required. As a result, Exchange matching programs must continue in the absence of a cost-effectiveness finding.

After careful evaluation of the data presented above, CMS intends to continue using the current matching program structure, which is less costly than the alternative, non-Hub structure and achieves the primary goals of providing a single streamlined application process and accurate eligibility determinations. While CMS intends to retain the existing matching program structure moving forward, necessary changes will be made as needed to keep the matching programs compatible with changes in program operations and data flow. This cost benefit analysis and the decision to retain the current matching structure should increase the public's trust in the participating agencies as careful stewards of taxpayer dollars.

Because the Exchange matching programs incur a net cost (i.e., do not demonstrate that the matching programs are likely to be cost-effective), the Exchange matching agreements should be worded to provide for data integrity board (DIB) approval to be based on the other benefits and mitigating factors described in this analysis and in each individual agreement. Specifically, the agreements should provide justification for each DIB's written determination that the cost benefit analysis is not required to demonstrate cost-effectiveness for Exchange matching.