COMPUTER MATCHING AGREEMENT
BETWEEN
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES
And
THE OFFICE OF PERSONNEL MANAGEMENT
For
VERIFICATION OF ELIGIBILITY FOR MINIMUM ESSENTIAL COVERAGE
UNDER THE PATIENT PROTECTION AND AFFORDABLE CARE ACT
THROUGH AN
OFFICE OF PERSONNEL MANAGEMENT HEALTH BENEFIT PLAN

CMS Computer Matching Agreement No. 2021-12
Department of Health and Human Services No. 2104

Effective Date - June 8, 2021
Expiration Date - December 7, 2022

I. PURPOSE, LEGAL AUTHORITIES, AND DEFINITIONS

A. Purpose

This Computer Matching Agreement (Agreement) establishes the terms, conditions, safeguards, and procedures under which the U.S. Office of Personnel Management (OPM) will provide information to the Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS). The terms and conditions of this Agreement will be carried out by authorized officers, employees, and contractors of OPM and CMS. OPM and CMS are each a "Party" and collectively "the Parties."

Under the authority of 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) (collectively, the PPACA) and the implementing regulations, CMS, in its capacity as the Federally-facilitated Exchange, and other Administering Entities (AEs) will use OPM's eligibility information to verify an Applicant's or Enrollee's eligibility for Minimum Essential Coverage (MEC) through an OPM Health

Benefits Plan. Eligibility for an OPM Health Benefits Plan which meets affordability standards usually precludes eligibility for financial assistance (including an advance payment of the premium tax credit (APTC) or cost sharing reduction (CSR), which are types of insurance affordability programs) for a Qualified Health Plan (QHP) through the Federally-facilitated or State-based Exchanges.

The Computer Matching and Privacy Protection Act of 1988 (CMPPA) (Public Law 100-503), amended the Privacy Act (5 U.S.C. § 552a) and requires the parties participating in a matching program to execute a written agreement specifying the terms and conditions under which the matching program will be conducted, CMS has determined that status verification checks conducted by AEs using the Enterprise Human Resources Integration (EHRI) data source Status File provided to CMS by OPM constitute a "matching program" as defined in the CMPPA.

CMS has entered into matching agreements with the following federal source agencies: I) Social Security Administration (SSA), 2) Department of Homeland Security (DHS), 3) Internal Revenue Service (IRS), 4) 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 Marketplaces. CMS designed the Federal Data Services Hub (Hub) to be a centralized platform for the secure electronic interface that connects all AEs and trusted data sources.

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.

The responsible component for CMS is the Center for Consumer Information & Insurance Oversight (CCIIO). HHS/CMS will serve as the Recipient Agency, and as such, is responsible for publishing the Federal Register notice required by 5 U.S.C. § 552a(e)(12). The OPM components responsible for the disclosure of information are the Human Capital Data Management and Modernization office and r the Office of the Chief Information Officer. OPM will serve as the Source Agency in this Agreement.

By entering into this Agreement, the Parties agree to comply with the terms and conditions set forth herein and the applicable law and implementing

regulations. The terms and conditions of this Agreement will be carried out by Authorized Users.

B. Legal Authorities

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

1. This Agreement is executed pursuant to the Privacy Act as amended (5 U.S.C. § 552a) and the regulations and guidance promulgated thereunder, including Office of Management and Budget (0MB) Circular A-108 "'Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act" published at 81 Federal Register (FR) 94424 (Dec. 23, 2016), and 0MB guidelines pertaining to computer matching published at 54 FR 25818 (June 19, 1989).

2. Under the PPACA, certain individuals are eligible for certain financial assistance in paying for private insurance coverage under a QHP when enrollment is through an Exchange. Such assistance includes APTC, under 26 U.S.C. § 36B and section 1412 of the Affordable Care Act, and CSRs under section 1402 of the Affordable Care Act.

3. Section 36B(c)(2) of the Internal Revenue Code of 1986, as added by 1401 of the PPACA, provides that an Applicant is ineligible for APTC if he or she is eligible for MEC as defined in 26 U.S.C. § 5000A(t) other than MEC described in 26 U.S.C. (t)(l)(C). Section 1402(t)(2) of the PPACA provides that an individual is ineligible for CSRs if the individual is not also eligible for the premium tax credit for the relevant month.

4. Section 1331 of the PPACA authorizes the Basic Health Program (BHP) and requires each state administering a BHP to verify whether an individual is eligible for certain MEC such as an OPM Health Benefits Plan (45 CFR § 155.320(d)).

5. Section 1411 of the PPACA requires the Secretary of HHS to establish a program to determine an individual's eligibility to purchase a QHP through an Exchange and to determine eligibility for APTC and CSRs. The system established by HHS under 1411(c)(4)(B) and (d) to determine eligibility for APTC and CSRs requires an Exchange to verify whether an individual is eligible for certain eligible employer sponsored plans, such as an OPM Health Benefits Plan (45 CFR § 155.320(d)), by OPM sending information

to HHS/CMS for HHS/CMS to provide the response to the requesting AE through the Hub.

6. Under 45 CFR §§ 155.302 and 155.305, the eligibility determinations for APTC and CSRs may be made by an Exchange or HHS. CMS carries out the Exchange-related responsibilities of HHS (76 Fed. Reg. 4703 (Jan. 26, 2011)).

7. Under the authority of sections 1311, 1321, and 1411(a) of the PPACA, the Secretary of HHS adopted the regulation at 45 CFR § 155.330, which further addresses the requirements for an Exchange to re-determine an Applicant's eligibility for enrollment in a QHP through an Exchange and for APTC and CSRs during the Benefit Year based on certain types of changes in circumstances.

8. The Privacy Act, 5 U.S.C. § 552a(b)(3), authorizes a Federal agency to disclose information about an individual that is maintained by an agency in an agency system of records, without the prior written consent of the individual, when such disclosure is pursuant to a routine use. OPM has published a routine use in its applicable system of records notice (SORN) to address the disclosures under this Agreement. CMS does not disclose information in its system of records to OPM as part of this Agreement.

C. Definitions

For the purposes of this Agreement:

1. " Administering Entity" or "AE" means a state Medicaid agency, Children's Health Insurance Program (CHIP), a Basic Health Program (BHP), or an Exchange administering an Insurance Affordability Program;

2. "Advance payments of the premium tax credit" or "APTC" is defined under 45 CFR § 155.20 to mean payment of the tax credit specified in§ 36B of the IRC (as added by§ 1401 of the PPACA) which are provided on an advance basis on behalf of an eligible individual enrolled in a QHP through an Exchange in accordance with§ 1412 of the PPACA. APTC is not considered Federal Tax Information under 26 U.S.C. § 6103;

3. "Applicant" means an individual who is seeking eligibility for him or herself through an application submitted to an Exchange, excluding individuals seeking eligibility for an exemption from the individual shared responsibility payment pursuant to subpart G of Part 155 of Title 45 CFR, submitted to a BHP program, or transmitted to an Exchange by an agency

administering an Insurance Affordability Program for at least one of the following (i) enrollment in a QHP through an Exchange; or (ii) the BHP;

4. "Authorized Representative" means an individual person or organization acting, in accordance with 45 CFR § 155.227, on behalf of an Applicant or Enrollee in applying for an eligibility determination, including a redetermination, and in carrying out other ongoing communications with the Exchange;

5. "Authorized User" means an information system user who is provided with access privileges to any data resulting from this match or to any data created as a result of this match. Authorized Users include AEs;

6. "Benefit Year" means the calendar year for which a health plan purchased through an Exchange provides coverage for health benefits;

7. "Breach" is defined by 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 or potentially accesses personally identifiable information (PII); or (2) an authorized user accesses or potentially accesses PII for other than authorized purposes;

8. "CMS" means the Centers for Medicare & Medicaid Services;

9. "Cost-sharing reduction" or "CSR" is defined at 45 CFR § 155.20 and means a reduction in cost sharing of an eligible individual enrolled in a silver level plan in the Exchange or for an individual who is an Alaskan Native/American Indian enrolled in a QHP in the Exchange. CSRs are not considered Federal Tax Information under 26 U.S.C. § 6103;

10. "Eligibility determination" means an AE's determination of an Applicant's eligibility for Insurance Affordability Programs, including a redetermination based on a self-reported change pursuant to 45 CFR § 155.330, and the process of appealing an eligibility determination when an appeal is provided pursuant to section 1411(f) of the PPACA;

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

12. "Exchange" may refer to the Federally-facilitated Exchange or a State-based Exchange, as applicable based on context;

13. " FFE" means Federally-facilitated Exchange, which is an Exchange established by HHS and operated by CMS under § 1321 of the PPACA;

14. "HHS" means the Department of Health and Human Services;

15. "Hub" or "Data Services Hub" is the CMS federally managed, single data exchange for AEs to use 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 agencies administering Insurance Affordability Programs for eligibility determination and enrollment services;

16. " Insurance Affordability Program" or "IAP" include: (1) a program that makes coverage in a QHP through an Exchange with APTC; (2) a program that makes available coverage in a QHP through an Exchange with CSRs; (3) the Medicaid program established under Title XIX of the Social Security Act; (4) the Children's Health Insurance Program (CHIP) established under Title XXI of the Social Security Act; and (5) the Basic Health Program (BHP) established under Section 1331 of the PPACA;

17. "Minimum Essential Coverage" or "MEC" is defined in IRC § 5000A(f), and includes health insurance coverage offered by a QHP and provided through an Exchange, an eligible employer-sponsored plan or government-sponsored coverage such as coverage under Medicare Part A, TRICARE, or a health plan under 22 U.S.C. § 2504(e) (relating to Peace Corps volunteers);

18. "OPM Health Benefits Plan" means a group insurance policy or contract, medical or hospital service agreement, membership or subscription contract, or similar group arrangement provided by a carrier for the purpose of providing, paying for, or reimbursing expenses for health services and as contracted for or approved by OPM under 5 U.S.C. Chapter 89;

19. "PPACA" means Patient Protection and Affordable Care Act of2010 (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);

20. "PII" or "personally identifiable information" is defined by 0MB Circular A 130, 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;

21. " Qualified Health Plan" or "QHP" is a health plan that has in effect a certification that it meets the standards described in subpart C of Part 156 of Title 45 of the Code of Federal Regulations issued or recognized by each Exchange through which such plan is offered in accordance with the process described in subpart K of Part 155 in Title 45 of the Code of Federal Regulations;

22. "Recipient Agency" as defined by the Privacy Act (5 U.S.C. *§* 552a(a)(9)) means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program, which will be Centers for Medicare & Medicaid Services;

23. "Record" is defined in the Privacy Act at 5 U.S.C. 552a(a)(4) and means any item , collection , or grouping of information about an individual that is maintained by an agency, including but not limited to information about the individual ' s education, financial transactions, medical history, and criminal or employment history and that contains the individual' s name, or the identifying number, symbol, or other identifying particular assigned to the individual;

24. "Security Incident" or "Incident" is defined by 0MB 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;

25. "Source Agency" as defined by the Privacy Act (5 U.S.C. *§* 552a(a)(l1)) and includes any agency that discloses records contained in a system of records to be used in a matching program. OPM is the Source Agency in this Agreement;

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

27. "Status File" is a file provided by OPM to CMS that includes data about an individual's Federal Employee's Health Benefit eligibility;

28. "System of Records" as defined by the Privacy Act (5 U.S.C. § 552a(a)(5)) means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

II. RESPONSIBILITIES OF THE PARTIES

I. CMS Responsibilities

a. CMS will develop procedures through which an Applicant or Enrollee may request an eligibility determination via a single, streamlined application.

b. CMS will receive a monthly Status File with all Federal employee health care insurance information from OPM.

c. AEs administering Insurance Affordability Programs will access the Status File through the Hub. The Hub will use the information contained in the OPM status file to indicate if an Applicant or Enrollee is enrolled or eligible for an OPM Health Benefits Plan, which is a form of MEC under the PPACA.

d. CMS will receive a Premium Spread Index File from OPM on an annual basis that identifies the lowest premium available to a Federal employee in each of the 32 premium localities.

e. AEs will receive data from the Premium Spread Index File when an individual is identified in the OPM Status file. The AE will use this data to determine whether the lowest cost self-only plan offered to the employee is affordable.

f. CMS has developed and will maintain procedures through which AEs can request and receive information verifying eligibility for MEC from the OPM Status File through the CMS Hub to make eligibility determinations.

g. CMS will enter into agreements with AEs that bind these entities to comply with appropriate privacy and security protections for PII,

including requirements for these entities and their employees, contractors, and agents to comply with privacy and security requirements that are consistent with section **1411**(g) of the PPACA, 45 CFR § 155.260, and the terms and conditions of this Agreement.

h. CMS will provide Congress and the 0MB with advance notice of this matching program, and upon completion of OMB's review, will publish the required matching notice in the Federal Register.

i. CMS will ensure the receipt of appropriate consents from Applicants or Enrollees for use of PII collected, used, and disclosed for the purposes and programs outlined in this Agreement.

2. OPM Responsibilities

a. OPM will provide CMS with data from the OPM system of records OPM/GOVT-1 (General Personnel Records), 77 Federal Register, 73694, December **11,** 2012. The disclosure to CMS is authorized by Routine Use "rr" . See https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf

b. OPM will submit the following to CMS: (1) a monthly Status File containing personnel data; and (2) an annual Premium Spread Index File, which gives information identifying the lowest premium available to a Federal employee in each of the thirty-two (32) OPM premium localities on an annual basis. The individual data elements contained in the monthly Status File sent from OPM to CMS are detailed in Section IV.B.2.

3. 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.

III. JUSTIFICATION AND ANTICIPATED RESULTS

A. Cost Benefit Analysis Requirements

As required by§ 552a(u)(4) of the Privacy Act, a cost benefit analysis (CBA) is included as Attachment 1, covering this matching program and seven other "Marketplace" matching programs which CMS conducts with other Federal agencies . The CBA demonstrates that monetary costs to operate all eight Marketplace matching programs exceed $39 million, but does not quantify direct governmental cost saving benefits sufficient to estimate whether they offset such costs. The CBA, therefore, does not demonstrate that the matching program is likely to be cost-effective and does not provide a favorable benefit cost ratio.

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 (Privacy Act of 1974: Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988).

B. Other Supporting Justifications

Even though the Marketplace matching 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 Data Integrity Board (DIB) approval of the matching programs.

1. Certain Marketplace matching programs are required (i.e., are based on a statutory obligation, not discretionary to conduct).

2. The Marketplace matching programs improve the speed and accuracy of consumer eligibility determinations while minimizing administrative burdens and achieving operational efficiencies.

3. The matching programs benefit the public and consumers by accurately determining consumers' eligibility for financial assistance including

APTC and CSRs.

4. The efficient eligibility and enrollment process provided by the Marketplace matching programs contributes to greater numbers of consumers enrolling in Marketplace qualified health plans, resulting in a reduction of the uninsured population and improving overall health care delivery.

5. 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 is no cost savings to conducting the Marketplace matching 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 matching program to the extent possible, and by using a matching program operational structure and technological process that is more efficient than any alternatives. CMS estimates that the cost of operating this computer match is about $39 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.

The Privacy Act does not require the showing of a favorable ratio for the match to be continued, only that an analysis be done unless statutorily exempted or waived by the DIB. 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.

IV. RECORDS DESCRIPTION

The Privacy Act at 5 U.S.C. § 552a(o)(l)(B) requires that each CMA specifically describe 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 program.

A. Systems of Records (SORs)

CMS

The CMS SORN that supports this matching program is the "CMS Health Insurance Exchanges System (HIX)," System No. 09-70-0560, published at 78 FR 63211 (October 23, 2013) and partially amended at 83 FR 6591 (February 14, 2018).

OPM

The OPM System of Records for this matching program is titled "General Personnel Records" (OPM\GOVT-1), published at 77 Federal Register, 73694 (December 11, 2012). The disclosure of information to CMS will be made in accordance with Routine Use "rr". See https://www.opm.gov/information-management/privacy- policy/sorn/opm- som-govt-1-general-personnel-records.pdf.

B. Specified Data Elements

1. From CMS to OPM. CMS will not share any data with OPM under this Agreement that will be used to support eligibility determinations. However, through the Hub, CMS will provide file transfer acknowledgements confirming that data files provided by OPM have transmitted successfully. If there is a transport level error during a file transmission, CMS will provide OPM with an automated error response to that effect. If, during the Hub's data validation process, CMS detects an error in a data file received from OPM, CMS will provide OPM with an error file.

2. From OPM to CMS. OPM will send a monthly, full refreshed Status File that contains a list of and data for, active Federal employees. The Status File will include the following specified data elements:

   a. Record type;
   b. Record number;
   C. Unique person ID;
   d. Social Security Number;
   e. Last name;
   f. Middle name;
   g. First name;
   h. Last name suffix;

1. Gender;
J. Date of birth; and
k. Health Plan Code.

3. OPM will also send to CMS, on an annual basis, a Premium Spread Index File that identifies the lowest premium available to a Federal employee in each of the 32 premium localities. The Premium Spread Index File provides premium data for the current and future calendar year, for both fee-for-service and health maintenance organization health plans , including the following specified data elements:

a. State;
b. Plan;
c. Option;
d. Enrollment code;
e. Current total bi-weekly premium;
f. Future total bi-weekly premium;
g. Future government pays bi-weekly premium;
h. Future employee pays bi-weekly premium
1. Future change in employee payment bi-weekly premium;
J. Current total monthly premium;
k. Future total monthly premium;
l. Future government pays monthly premium;
m. Future employee pays monthly premium;
n. Future change in employee payment monthly premium.

C. Number of Records

CMS will receive a bulk file from OPM annually for the Premium Spread Index File, and monthly for the Status File. The files will contain data elements for all individuals currently covered by or eligible for OPM health coverage. OPM estimates that each file will contain data elements relevant to approximately two million individuals.

D. Projected Starting and Completion Dates of the Matching Program

Starting Date - June 8, 2021

Completion Date - December 7, 2022 (December 7, 2023 if renewed for 1 year).

V. NOTICE PROCEDURES

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

B. At the time of application or change of circumstances, an AE administering an Insurance Affordability Program will provide a notice to the Applicants or Enrollees about the OMB-approved streamlined eligibility application.

C. The AE administering the Insurance Affordability Program will ensure provision of a redetermination notice in accordance with applicable law. These notices will inform Applicants and Enrollees that the information they provide may be verified with information in the records of other Federal agencies.

VI. VERIFICATION PROCEDURES AND OPPORTUNITY TO CONTEST FINDINGS

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

Before an AE may take any adverse action based on the information received from the matches under this Agreement, the AE will permit the individual to provide the necessary information or documentation to verify eligibility information. When an agency administering an Insurance Affordability Program determines that an Applicant or an Enrollee is ineligible for an Insurance Affordability Program based on the information provided by the match, and that information is inconsistent with information provided on the streamlined eligibility application or otherwise by an Applicant or Enrollee, the agency administering the Insurance Affordability Program will comply with applicable law and will notify each Applicant or Enrollee of the match findings and provide the following information: (1) the agency received information that indicates the Applicant or Enrollee is ineligible for an Insurance Affordability Program; and
(2) the Applicant or Enrollee has a specified number of days from the date of the notice to contest the determination that the Applicant or Enrollee is ineligible for the relevant Insurance Affordability Program.

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 will be provided the opportunity to follow the procedures outlined in 45 CFR §§ 155.315 and 155.320. The AE will provide the proper contact information and instructions to the individual resolving the inconsistency.

2. If the AE is an agency administering a Medicaid or CHIP program, an individual seeking to resolve inconsistencies between attestations and the results of electronic for the purposes of completing an Eligibility Determination will be provided the opportunity to follow the procedures outlined in 42 CFR §§ 435.945 through 435.956. The AE will provide the proper contact information and instructions to the individual resolving the inconsistency.

3. Per 42 CFR § 600.345, if the AE is a BHP, it must elect either the Exchange verification procedures set forth in VI.B.1 or the Medicaid /CHIP verification procedures set forth at VI.B.2.

VII. ACCURACY ASSESSMENTS

OPM currently estimates that 99% of the information is accurate for PPACA purposes in cases where: (I) an exact Applicant match is returned, (2) the Applicant has an enrollment status of "verified," and (3) the Applicant's enrollment period coincides with the dates received from the Hub.

VIII. DISPOSITION OF MATCHED ITEMS

These procedures are required by the Privacy Act at 5 U.S.C. §552a(o)(l)(F):

CMS will retain electronic records that contain verified Applicant, Beneficiary, or Enrollee information for a period of ten (10) years to the extent that a match results in an inconsistency, in accordance with retention schedule DAA-0440-2014-0003 which was approved by NARA May 4, 2016. The retained electronic records will reflect the results of the match in order to meet legal evidentiary requirements. Retained records will not contain raw OPM data received via the Hub. The source data provided to CMS from OPM will be overwritten approximately every thirty days as OPM provides updated files.

CMS will dispose of data in accordance with their applicable disposition schedules. CMS will not create permanent files or a separate system comprised solely of the data provided by the other Party.

IX. SECURITY PROCEDURES

A. General. Both CMS and OPM will maintain a level of security needed to protect the information contained on the system with the highest appropriate sensitivity level. The System Security Level for the Hub (FDSH) and the FFE is FISMA Moderate (as are all ACA/Exchange systems). The information classification is Sensitive, but not Classified (regarding PII).

B. Legal Compliance. Both Parties shall comply with the limitations on use and disclosure, storage, transport/transmission, retention, and safeguarding of data under all applicable Federal laws and regulations. These laws and regulations include 141 l(g) of the PPACA, the Privacy Act of 1974, as amended (5 U.S.C. § 552a); the E-Government Act of 2002, which includes the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §§ 3541-3549, as amended by the Federal Information Security Modernization Act, 44 U.S.C. §§ 3551-3558; HIPAA; the Computer Fraud and Abuse Act of 1986; the Clinger-Cohen Act of 1996; and the corresponding implementation regulations for each statute.

CMS and OPM will comply with applicable 0MB circulars and memoranda, including 0MB Circular A-130, Managing Information as a Strategic Resource, published at 81 FR 49689 (July 28, 2016); applicable National Institute of Standards and Technology (NIST) directives and publications; and the Federal Acquisition Regulations. These laws, directives, and regulations include requirements for safeguarding Federal information systems and PII used in Federal agency business processes, as well as related reporting requirements. The Parties recognize and will implement the laws, regulations, NIST standards, and 0MB directives including those published subsequent to the effective date of this Agreement.

C. FISMA Compliance. FISMA requirements apply to all Federal contractors, organizations, or entities that possess or use Federal information, or that operate, use, or have access to Federal information systems on behalf of an agency. Both parties are responsible for oversight and compliance of their contractors and agents.

D. Incident Reporting, Potential Loss, and Breach Notification. CMS will comply with 0MB reporting guidelines in the event of a loss, potential loss, security incident, or breach of PII (hereafter referred to as "incident"). (See

0MB M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (Jan. 3, 2017), and 0MB M-20-04, Fiscal Year 2019-2020 " Guidance on Federal Information Security and Privacy Management Requirements" (Nov. 19, 2019).) When CMS experiences the incident will notify OPM' s System Security Contact named in this Agreement within one (1) hour of discovering the incident. If CMS is unable to speak with OPM' s System Security Contact within one (1) hour or if for some reason contacting the System Security Contact is not practicable (e.g., outside of normal business hours), then the following contact information will be used:

- The OPM Security Operations Center at 844-377-6109 or Cybersolutions@opm.gov.

The Party that experienced the incident will be responsible for following its established procedures, including notifying the proper organizations (e.g., United States Computer Emergency Readiness Team (US-CERT)), conducting a breach and risk analysis, and making a determination of the need for notice and/or remediation to individuals affected by the loss. The Parties under this agreement will follow PII breach notification policies and related procedures as required by 0MB guidelines and the US-CERT Federal Incident Notification Guidelines. If the party experiencing the incident determines that the risk of harm requires notification to the affected individuals or other remedies, then that party will carry out these remedies with consultation from the other party but without cost to the other party.

E. Administrative Safeguards. Both Parties will comply with the existing and future requirements set forth in the laws, directives, and regulations referenced in the preceding subsections and any applicable amendments published after the effective date of this Agreement. These laws, directives and regulations include requirements for safeguarding Federal information systems and personally identifiable information used in Federal agency business processes, as well as related reporting requirements. Specifically, FISMA requirements apply to all Federal contractors, organizations, or entities that possess or use Federal information, or that operate, use, or have access to Federal information systems on behalf of an agency. Both Parties agree that personnel with access to the data matched and created by the match receive training to ensure proper verification in a manner consistent with this agreement. Accordingly, both Parties will restrict access to the matched data and to

any data created by the match to only those authorized users of the CMS Hub who need it to perform their official duties in connection with the uses of data authorized in this Agreement. Further, both Parties will advise all personnel who will have access to the data matched and to any data created by the match of the confidential nature of the data, the safeguards required to protect the data, regulations applicable to retention of the data, and the civil and criminal sanctions for noncompliance contained in the applicable Federal laws.

F. Physical Safeguards. CMS will store the data received and any data created by the match in an area that is physically and technologically secure from access by unauthorized persons at all times. Physical safeguards may include door locks , card keys, biometric identifiers, etc. Those records will be maintained under conditions that restrict access to persons who need them in connection with their official duties related to the matching process. Only authorized personnel will transport the data matched and any data created by the match. It is the responsibility of the user's supervisor to ensure that both Parties are notified when a user has departed or duties have changed such that the user no longer needs access to the system, to ensure timely deletion of the user's account and password.

G. Technical Safeguards. Both Parties will process any data under this Agreement under the immediate supervision and control of the authorized users 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. CMS will also ensure that only authorized users have access to the data and will protect the confidentiality of the data. CMS will provide training to the authorized users on the usage of the system and the data.

H. Application of Policies and Procedures. Both Parties will adopt policies and procedures to ensure that each Party uses the information obtained under this Agreement and retained in their respective records or obtained from each other is used solely as provided in this Agreement. Both Parties will comply with these policies and procedures and any subsequent revisions.

I. Security Assessment. NIST Special Publication 800-37, Revision 1, encourages agencies to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information. NIST 800-37 further encourages that this type of reciprocity is best achieved when agencies are transparent and

make available sufficient evidence regarding the security state of an information system so that an authorizing official from another organization can use that evidence to make credible, risk-based decisions regarding the operation and use of that system or the information it processes, stores, or transmits. Consistent with that guidance, the Parties agree to make available to each other upon request system security evidence for the purpose of making risk-based decisions. Requests for this information may be made by either Party at any time throughout the duration or any renewal of this Agreement.

J. Compliance. CMS must ensure information systems and data exchanged under this matching agreement are maintained compliant with CMS Acceptable Risk Safeguards (ARS) standards. The ARS document can be found at: https://www.cms.gov/Research-Statistics-Data-and-Systems /CMS- Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-ltems/STANDARD-ARS-Acceptable-Risk-Safeguards. To the extent, these documents are revised during the term of this Agreement, CMS must ensure compliance with the revised version.

X. RECORDS USAGE, DUPLICATION, AND REDISCLOSURE

CMS and OPM will comply with the following limitations on use, duplication, and disclosure of the electronic files, and data provided by the other Party under this Agreement (the Data):

A. CMS will not use or disclose the Data for any purpose other than the purposes authorized by this Agreement or required under applicable Federal law , without the consent of the other party.

B. CMS will not duplicate or disseminate the other Party's Data, within or outside their respective agencies, without the written consent of the other party, except as required by Federal law or for purposes under this Agreement. CMS will ensure that AEs using the Hub will not duplicate or disseminate the submission and response files within or outside of their respective agencies, without the written consent of OPM, except as where required by law, under this Agreement. To gain consent for a use or disclosure of the Data that is not authorized by this Agreement, the agency requesting the consent must specify in writing at least the following: (I) the data to be used or disclosed, (2) to whom the data will be disclosed, (3) the reasons justifying such use or disclosure, and (4) the intended use of the data. Where duplication or dissemination is required by law, CMS will notify OPM of the disclosure.

C. CMS will not use the Data to extract information concerning individuals therein for any purpose not specified by this Agreement or allowed by applicable Systems of Records Notices (SORN) or Federal law.

D. Through the Hub, CMS may disclose the Data received from OPM to Exchanges and AEs pursuant to separate Computer Matching Agreements that authorize such entities to use the Data for eligibility determinations regarding APTC, CSRs and BHP. Exchanges, including CMS in its capacity performing eligibility determinations for the FFEs and State-based Exchanges who rely on CMS for eligibility and enrollment functions, and agencies administering BHPs may share the results of the data matches under this Agreement with Applicants or Enrollees; Application Filers; and the Authorized Representatives of such persons.

E. Any individual , including officers, employees, and contractors of the Parties 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 **141**l(g) of the PPACA are subject to the civil penalty provisions of **1411** (h)(2) and 45 CFR § 155.285, which carries a fine of up to $25,000 per use or disclosure.

XI. COMPTROLLER GENERAL ACCESS

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

XII. REIMBURSEMENT/FUNDING

All work performed by OPM to carry out the matching program under this Agreement will be performed on a reimbursable basis. OPM will allocate sufficient funds annually to support the completion of its responsibilities under this Agreement. The legal authority for transfer of funds is the Economy Act at 31 U.S.C. § 1535. Reimbursement will be transacted by means of a separate reimbursement instrument in accordance with the established procedures that apply to funding reimbursement actions. CMS and OPM will execute and maintain a separate Interagency Agreement on an annual basis to address CMS reimbursement of relevant OPM costs related to requests covered by this Agreement.

XIII. DURATION OF AGREEMENT

A. Effective Date:

The Effective Date of this Agreement is June 8, 2021, provided that CMS reported the proposal to re-establish this matching agreement to the Congressional committees of jurisdiction and 0MB in accordance with 5 U.S.C. § 552a(o)(2)(A) and (r) and 0MB Circular A-108 and, upon completion of their advance review period, CMS published notice of the matching program in the Federal Register for a minimum of thirty days as required by 5 U.S.C. § 552a(e)(l2).

B. Term: This initial term of this Agreement will be eighteen (18) months.

C. Renewal: The parties may, within three (3) months prior to the expiration of this Agreement, renew this Agreement for a period not to exceed one additional year if CMS and OPM certify the following to their DIB:

1. The matching program will be conducted without change; and

2. The parties have conducted the matching program in compliance with this Agreement.

D. Modification: The parties may modify this Agreement at any time by a written modification, mutually agreed to by both parties, provided that the change is not significant. A significant change would require a new agreement.

E. 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.

XIV. 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 OPM and CMS for the purposes described in this Agreement. CMS and OPM 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.

XV. PERSONS TO CONTACT

The OPM contacts are:

1. IT Security Issues

   Darrin McConnell

   Office of the Chief Information Officer
   U.S. Office of Personnel Management 1900
   E Street
   Washington, DC 20415
   Phone: (202) 606-6210
   E-Mail: Darrin.McConnell@opm.gov

2. Privacy Act Agreement Issues

   Kellie Cosgrove Riley
   Senior Agency Official for Privacy
   U.S. Office of Personnel Management
   1900 E Street, NW
   Washington , DC 20415
   Phone: (202) 606-2308
   E-Mail: Kellie.Riley@opm.gov

3. Data Issues

   Abbas Malekghassemi, Program Manager (Acting)
   Data Standards, Management, and Modernization (DSMM) Office of Human Capital Data Management and Modernization (HCDMM)U.S. Office of Personnel Management 1900 E. Street, Washington, DC 20415
   Phone: (202) 418-3369
   E-Mail: <Abbas.Malekghassemi@opm.gov>

The CMS contacts are:

1. Program Issues

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. Medicaid/CHIP Issues

Julie Boughn
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: S2-23-06
Baltimore, MD 21244-1850
Telephone: (410) 786-9361
Fax: (443) 796-5622
Email: Julie.Boughnl@cms.hhs.gov

3. Systems Security

Darrin V. Lyles
Security and Privacy Technical Advisor
Marketplace Information Technology Group
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244
Telephone: (410) 786-4744
Telephone: (443) 979-3169 (Mobile)
Email: Darrin.Lyles@cms.hhs.gov

4. Privacy and Agreement Issues

Barbara Demopulos, Privacy Advisor
Division of Security, Privacy Policy & Governance
Information Security & Privacy Group
Office of Information Technology
Centers for Medicare & Medicaid Services
Location: Nl-14-40
7500 Security Boulevard
Baltimore, MD 21244-1850
Telephone: (410) 786-6340
Email: Barbara.demopulos@cms.hhs.gov

XVI. APPROVALS

A. Centers for Medicare & Medicaid Services Program Official

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.

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.

Jeffrey Grant -S Digitally signed by Jeffrey Grant -S
Date: 2021.02.18 13:25:44 -05'00'

Jeffrey D. Grant
Acting Director

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

Date_____

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

Karen M. Shields -S

Digitally signed by Karen M. Shields -S
Date: 2021.02.18 08:34:54 -05'00'

Karen Shields
Deputy Director

Center for Medicaid and CHIP Services
Centers for Medicare & Medicaid Services

Date 2-18-2021

C. Centers for Medicare & Medicaid Services Approving Official

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.

Michael E. Pagels-S

Digita lly signed by Michael E. Pagels-S
Date: 2021.02.18 16:41:53 -05'00'

Michael Pagels
Director
Division of Security Privacy Policy and Governance, and
Senior Official for Privacy
Information Security and Privacy Group
Office of lnformation Technology
Centers for Medicare & Medicaid Services

Date_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

D. Office of Personnel Management Approving Official

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.

LANCE HARRIS

Digitally signed by LANCE HARRIS
Date: 2021.02.17 15:17:27 -05'00'

Lance Harris, Manager, Data Support and Analysis, signing for David Padrino.

David Padrino
Executive Director, Human Capital Data Management and Modernization
U.S. Office of Personnel Management

Date_____

XVII. DATA INTEGRITY BOARD APPROVALS

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

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.

The authorized DIB official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, confirm that nonverbal agreements of any kind shall be binding or recognized, and hereby commits their respective organization to the terms of this Agreement.

James B. Duncan -S

Digitally signed by James B. Duncan -S
Date: 2021.03.17 15:12:32 -04'00'

Blair Duncan
Acting Chairperson, HHS Data Integrity Board
U.S. Department of Health and Human Services

Date_____

B. Office of Personnel Management Data Integrity Board Official

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.

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

KELLIE RI Digitally signed by KELLIE RILEY

Kellie Cosgrove Riley
Senior Agency Official for Privacy
Chairperson, OPM Data Integrity Board
Office of Personnel Management

Date_____

Attachment 1: Cost-Benefit Analysis