

**COMPUTER MATCHING AGREEMENT
BETWEEN
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES
AND
THE DEPARTMENT OF HOMELAND SECURITY
UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES
FOR THE
VERIFICATION OF UNITED STATES CITIZENSHIP AND IMMIGRATION
STATUS DATA FOR ELIGIBILITY DETERMINATIONS**

**CMS Computer Matching Agreement No. 2021-10
Department of Health and Human Services No. 2010**

Effective Date: April 20, 2021
Expiration Date: October 19, 2022

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 of Homeland Security (DHS), United States Citizenship and Immigration Services (USCIS) will engage in a matching program with the Department Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS) (hereinafter “the Parties”) to assist CMS and authorized State Administering Entities (collectively called “AEs”), through the Data Services Hub (“the Hub”), in making eligibility determinations under the Patient Protection and Affordable Care Act (Public Law (Pub. L.) No. 111-148), as amended by the Health Care and Education Reconciliation Act of 1010 (Pub. L. No. 111-152) (collectively, the PPACA) and its implementing regulations. The AEs will use the USCIS information in determining individuals’ eligibility to enroll in a Qualified Health Plan (QHP) through an Exchange, in an Insurance Affordability Program (IAP), and for Exemptions.

USCIS will provide CMS with specific USCIS data through the DHS/USCIS Systematic Alien Verification for Entitlements (SAVE) Program, which provides immigration status and naturalized or derived citizenship data to authorized federal, state, and local agencies to use in ensuring that only those Applicants or Enrollees who are eligible receive benefits. Specifically, USCIS will provide CMS with electronic access to immigrant, nonimmigrant, and naturalized or derived citizenship (in certain circumstances) information.

Access to this information will assist CMS and AEs in determining whether an Applicant is lawfully present, a qualified non-citizen, or a naturalized or derived citizen, and whether the 5-year waiting period, 7-year limit or CHIPRA 214 exemptions for many non-citizens applies and has been met in order to determine whether the individual is eligible for enrollment in a QHP or IAP or for one or more Exemptions.

The Privacy Act of 1974, as amended (5 U.S.C. §552a), requires the Parties participating in a

matching program to execute a written agreement specifying the terms and conditions under which the matching will be conducted. CMS has determined that immigration status verifications conducted through the Hub using the SAVE Program constitutes a "matching program" as defined at 5 U.S.C. §552a(a)(8).

The responsible component for CMS is the Center for Consumer Information & Insurance Oversight (CCIIO). CMS will serve as the Recipient Agency in this matching program and will be responsible for publishing the Federal Register (FR) Notice required by 5 U.S.C. §552a(e)(12). DHS/USCIS is the Source Agency. The responsible DHS component is USCIS.

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

B. Legal Authorities

The following statutes and regulations govern or provide legal authority for the uses and disclosures of data to be made 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 (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).
2. This Agreement is executed to implement certain health care reform provisions of the PPACA codified at 42 U.S.C. §18001 et seq., and implementing regulations at 42 Code of Federal Regulations (CFR) Parts 431, 435, 457, and 45 CFR Parts 155-157.
3. Section 1312(f)(3) of the PPACA specifies that to be eligible to enroll in a QHP through the Exchange, an individual must be a United States Citizen or a national or be a non-citizen who is lawfully present. To be eligible for an IAP (which includes advance payments of the premium tax credit (APTC) and cost-sharing reductions (CSRs)), an individual must be a United States Citizen or a national or be a non-citizen who is lawfully present. 26 U.S.C. § 36B(c)(1) and (e); 42 U.S.C. § 18071(e). *See also* 45 CFR §§155.305(f) and (g).
4. Section 1943(b) of the PPACA (as added by section 2201 of the PPACA) requires that Medicaid and Children's Health Insurance Program (CHIP) agencies utilize the same streamlined enrollment system and secure electronic interface established under section 1413 of the PPACA to verify eligibility.
5. Section 1411(c)(2)(B)(ii) of the PPACA provides that the Secretary of HHS will transmit the following identifying information to the Secretary of DHS for a determination as to whether the information is consistent with information in the records of DHS: name, date of birth, and any identifying information with respect to an individual's immigration status provided under PPACA subsection 1411(b)(2), for the purposes of verifying citizenship and immigration status.
6. Section 102 of the Homeland Security Act of 2002, 6 U.S.C. § 112, and section 103 of

the Immigration and Nationality Act (INA), 8 U.S.C. § 1103, vest the Secretary of Homeland Security with administration of the immigration and naturalization laws of the United States.

7. The Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 100 Stat. 3359, as amended (IRCA), requires the former Immigration and Naturalization Service (currently USCIS, within DHS, effective March 1, 2003) to establish a system for verifying the immigration status of non-citizen Applicants for, and recipients of, certain types of federally funded benefits, and to make the system available to federal, state and local benefit-issuing agencies and institutions that administer such benefits.

8. The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Pub. L. No. 104-208, 110 Stat. 3009, as amended, requires that the former Immigration and Naturalization Service (currently USCIS, within DHS, effective March 1, 2003) respond to an inquiry by a federal, state, or local agency seeking to verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law.

9. Section 213A of the INA, codified at 8 U.S.C. §§ 1183a and 1631, DHS implementing regulations found at 8 C.F.R. Part 213a, and the Form I-864 and its Instructions, provide details on the applicability and enforcement of the Form I-864 Affidavit of Support, as well as consent language authorizing the use and agency sharing of sponsorship information.

10. 26 U.S.C. §6103(l)(21) authorizes the disclosure of certain tax return information as defined under 26 U.S.C. §6103(b)(2) (hereinafter "return information") for purposes of determining eligibility for certain IAPs 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 IAPs.

11. Sections 1137(d) and 1902(a)(7) of the Social Security Act, codified at 42 U.S.C. §§ 1320b-7(d) and 1396a(a)(7), permit the sharing of certain immigration information to determine eligibility under the Medicaid state plan through SAVE. Section 1902(a)(7) of the Act permits Medicaid state plans to use or disclosure information concerning applicants and recipients to SAVE for purposes directly connected with the administration of the plan. 42 C.F.R. § 431.302(a) defines "purposes directly connected with the administration of the plan" as including "establishing eligibility," "determining the amount of medical assistance," or "conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan."

C. Definitions

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

2. "Applicant" means an individual seeking an Eligibility Determination for enrollment in a QHP through an Exchange, an IAP or a certification of Exemption; this term includes individuals whose eligibility is determined at the time of a renewal or redetermination;

3. "APTC" or advance payment of the premium tax credit means payment of the tax

credits specified in section 368 of the Internal Revenue Code of 1986 (as added by section 1401 of the PPACA), which are provided on an advance basis to an eligible individual enrolled in a QHP through an Exchange in accordance with sections 1411 and 1412 of the PPACA;

4. "Breach" is defined by OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (PII) (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 or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose;

5. "CHIP" or the Children's Health Insurance Program means the state program established under Title XXI of the Social Security Act;

6. "CMS" means the Centers for Medicare & Medicaid Services; the agency oversees many federal healthcare programs, in addition to programs that involve health information technology;

7. "CSRs" or Cost Sharing Reductions means cost sharing reductions for 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;

8. "DHS" means the Department of Homeland Security;

9. "Eligibility Determination" means the determination of eligibility by an AE for enrollment in a QHP through an Exchange, an IAP or for certifications of Exemption. This refers to initial determinations or redeterminations based on a change in the individual's status, and appeals;

10. "Exemption" means an exemption from the requirement or penalty imposed by section 5000A of the IRC - pursuant to section 1311(d)(4)(H) of the PPACA, an Exchange, subject to section 1411 of the PPACA, must grant a certificate of exemption attesting that an individual is exempt from the individual responsibility requirement or penalty imposed by section 5000A of the IRC;

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

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

13. "Hub" or "Data Services Hub" is the CMS-managed electronic service to interface among connecting entities and refers to both the web services connection to various agencies providing verification services and a system that will apply system logic to transmit the data it receives with respect to eligibility;

14. "Minimum Essential Coverage" or "MEC" is defined in the Internal Revenue Code (IRS) §5000A(f) and includes health insurance coverage offered in the individual market within a state, which includes a QHP offered through an Exchange, an eligible

employer-sponsored plan, or government-sponsored coverage such as coverage under Medicare Part A, TRICARE, or a Health Care Program;

15. "PPACA" means Patient Protection and Affordable Care Act (Public Law No. 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Pub. L. No. 111-152), codified at 42 U.S.C. 18001 et seq. (collectively, the PPACA);

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

17. "Security Incident" means "Incident," which is defined by OMB Memorandum M-17-12 Preparing for and Responding to a Breach of Personally Identifiable information (January 3, 2017) as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;

18. "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;

19. "USCIS" means United States Citizenship and Immigration Services, a component of DHS;

20. "USCIS Number" is the 9-digit United States Citizenship and Immigration Services number listed on the front of Permanent Resident Cards (Form I-551) issued after May 10, 2010, and it is the same as the Alien Registration Number;

21. "VIS" means "Verification Information System" a composite information system incorporating immigration data, as well as naturalized and derived citizenship data, from DHS data repositories and other federal databases. For more information, please see the following system of records notice: DHS/USCIS-004 "Systematic Alien Verification for Entitlements Program," 85 FR 31798 (May 27, 2020).

II. RESPONSIBILITIES OF THE PARTIES

A. CMS Responsibilities

1. CMS agrees to provide USCIS with the following information for the purpose of immigration status or naturalized/derived citizenship verification: Alien Registration Number, I-94 number, or other identifiers as defined in the records description in Section IV of this Agreement, as applicable, of the Applicant or Enrollee seeking an Eligibility Determination.

2. CMS, through the Hub, may disclose to AE the data received from USCIS under this Agreement for the purpose of determining eligibility for enrollment in a QHP through an Exchange, one of the IAPs, or an Exemption.

3. CMS, through the Hub, may request verification for individuals currently enrolled whose immigration status has an expiration date or condition.
4. CMS will notify the USCIS Safeguards and Recordkeeping Procedures Contact immediately whenever there is reason to believe a violation of this Agreement has occurred.
5. Consistent with National Institute of Standards and Technology (NIST) Special Publication 800-37, as revised, CMS will make available upon request system security assessments and other evidence for the purpose of making risk-based decisions, to the extent feasible and permitted by law. USCIS may request this information at any time throughout the duration or any extension of this agreement.
6. CMS shall allow USCIS to monitor and review all records and documents under CMS possession and control, or to which CMS has access or review rights, related to the use, abuse, misuse, discriminatory use, fraudulent use or improper use of USCIS verification data by AEs or their agents, including, but not limited to notice documents required by the Privacy Act or other applicable authority.
7. CMS shall provide USCIS with data and information regarding operation of the data services Hub for USCIS monitoring and compliance purposes, including data and information identifying the number and category of benefits (Medicaid, CHIP, QHP or BHP) by state or AE. CMS shall also provide USCIS with the opportunity to submit questions as necessary for appropriate monitoring and compliance purposes. CMS shall provide this data and information to USCIS, and an opportunity to submit questions, on an annual basis and otherwise as frequently as agreed upon between the Parties, but not later than 30 days after USCIS makes a written request for the information. CMS shall also cooperate and collaborate with USCIS in engaging with AEs to ensure that they comply with SAVE training requirements and, in the event of non-compliance, suspending or terminating AE access to SAVE through the Hub.
8. CMS shall cooperate and collaborate with USCIS and consider its input and recommendations when CMS monitors and oversees access through the Hub by CMS, AEs and their respective agents to the SAVE system. CMS will support USCIS direct assistance to verification system users (i.e., CMS, AEs and their respective agents) when necessary to ensure compliance with the terms of this Agreement. CMS shall take corrective measures in a timely manner to address all lawful requirements and recommendations within the scope of CMS' authority on every written USCIS finding including but not limited to misuse of the system, discriminatory use of the system, non-compliance with the terms, conditions and safeguards of this Agreement, USCIS program procedures or other applicable law, regulation or policy.
9. CMS shall allow DHS and its components to monitor CMS and CMS sub-user system access and usage of SAVE and to assist verification system users and sub-users, Agents or designees as necessary to ensure compliance with the terms of this Agreement by CMS, AEs, and their respective agents. USCIS shall be allowed to conduct compliance assistance activities, in coordination with CMS' primary oversight and monitoring processes, to review AEs' and their respective agents' compliance with this agreement. CMS shall take corrective measures within a timeframe agreed to by CMS and USCIS, to address all lawful requirements and recommendations within the scope of CMS' authority under 45 CFR § 155.1200 on every written USCIS finding including but not limited to those regarding waste, fraud, and abuse, discrimination or any misuse of the system, non-

compliance with the terms, conditions and safeguards of this Agreement, USCIS program policies and procedures or other applicable law or regulation.

10. CMS will enter into, and will provide USCIS with copies of, agreements with AEs that bind the AE, including their employees and contractors, to comply with the privacy and security requirements set forth in this Agreement, with the verification requirements at Section VI(A)(3) of this Agreement, and with USCIS's privacy and security requirements in conducting the verifications, and with all other requirements set forth in this Agreement. Additionally, when collection, use, or disclosure of data is otherwise required by law, an Exchange must, pursuant to 45 CFR § 155.260, require the same or more stringent privacy and security standards as a condition of contract or agreement with individuals or entities that;

- a. Gain access to PII submitted to an Exchange; or
- b. Collect, use or disclose PII gathered directly from Applicants or Enrollees while performing the functions outlined in the agreement with the Exchange.

11. CMS will enter into and will provide USCIS with copies of agreements prior to providing data to State Medicaid and CHIP agencies, under which such agencies agree to comply with the requirements which relate to the safeguarding of information about Applicants and Enrollees.

12. CMS will advise AEs that connect to SAVE via the verify lawful presence (VLP) Web Services interface to transition their systems to the most recent version of a SAVE release within 12 months from when the CMS Hub completes implementation of the latest version of the interface control agreement (ICA) in a VLP release, or they may experience technical difficulties.

13. When both respective DIBs have approved this Agreement, CMS will submit a report of the Matching Program to OMB and to the appropriate Committees of Congress for review and will provide a copy of such notifications to USCIS.

B. USCIS Responsibilities

1. USCIS agrees to make available the SAVE Program to CMS as an electronic method for determining whether Applicant information submitted by the Secretary of HHS to the Secretary of DHS pursuant to PPACA sections 1411(c)(2)(B) and 1413 is consistent with information available through the USCIS VIS.

2. USCIS agrees to provide the Hub with a response on each inquiry, as appropriate, to enable AEs to confirm whether the biographic, citizenship and immigration status information submitted by the Hub to SAVE is consistent with information available through the USCIS VIS.

3. USCIS agrees to provide CMS with training materials required for the use of the SAVE Program.

4. USCIS agrees to provide a sufficient number of primary verification user codes to assure the effective implementation of the verification procedures and instructions for obtaining necessary system access codes.

5. USCIS agrees to provide assistance to CMS and other AEs on policies and procedures

for participating in the SAVE Program, including technical instructions for accessing the system, requirements for safeguarding information contained in the system, proper and nondiscriminatory use of the system, and restrictions on retention and disclosure of system information. USCIS also agrees to provide CMS with the name, address and telephone number of an appropriate point of contact (POC) within USCIS, or its contractor organization, who can be contacted regarding any billing questions, as appropriate, or problems which arise in connection with CMS' participation in the verification program.

6. USCIS will conduct an additional verification search of available databases when an electronic request for additional verification is submitted. All AEs consent to electronic-only submission of all verification requests and additional information, including information submitted for additional verification (formerly submitted on paper Form G-845 and G-845 Supplement). SAVE will reject non-electronic (i.e., paper) verification requests and information submissions.

7. USCIS will advise the AE through the Hub or the AE's direct SAVE access method, as appropriate, if USCIS is unable to verify the Applicant's immigration status, at which time the AE may submit an electronic copy of the Applicant's immigration document or follow second, and if necessary, third step verification prompts.

8. An AE can submit an initial verification request to SAVE through the CMS hub and then, if needed, continue the case through the agency's direct connection with SAVE. USCIS will collaborate with CMS to address any information security and other matters associated with enabling this functionality.

III. JUSTIFICATION AND ANTICIPATED RESULTS

As requested by 5 U.S.C. §552a(o)(1)(B), the justification for the program and the anticipated results, including a specific estimate of any savings, is described below:

A. Cost Benefit Analysis Requirements

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 CMA with DHS and seven other "Marketplace" matching programs which CMS conducts with other federal agencies and the AEs. 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 in Section B. 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 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. 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)(1)(C) requires that each CMA specify a description of the records that will be matched, including a sample of data elements that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the program.

A. Systems of Records (SORs)

1. The CMS System of Record Notice (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). Routine Use 3 supports CMS's disclosures to DHS/USCIS: "To disclose information about Applicants and Relevant individual(s) in order to obtain information from other federal agencies and state agencies and third party data sources that provide information to CMS,

pursuant to agreements with CMS, for purposes of determining the eligibility of Applicants to enroll in QHPs through an Exchange, in insurance affordability programs, or for a certification of exemption from the individual responsibility requirement.”

2. The USCIS SORN that supports this data Matching Program is DHS/USCIS-004 “Systematic Alien Verification for Entitlements Program,” published at 85 FR 31798 (May 27, 2020). Routine Use I permits USCIS’s disclosure of information to CMS; it authorizes disclosures “to approved federal, state, and local governments agencies for any legally mandated purpose in accordance with their authorizing statute or law and when an approved Memorandum of Agreement or Computer Matching Agreement (CMA) is in place between DHS and the entity.”

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 a sample of data elements that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the program.

B. Number of Records

CMS estimates that approximately 6 million records may be transacted through SAVE queries for the purpose of determining eligibility for coverage in QHP and IAPs in calendar year 2021.

C. Specific Data Elements Used in the Match

1. From the CMS to USCIS. CMS will submit data elements pertaining to Applicants or Enrollees through SAVE to the USCIS VIS. These data elements may include the following:

- a. Last Name
- b. First Name
- c. Middle Name
- d. Date of Birth
- e. One or More Immigration Number (e.g. Alien Registration / USCIS Number, Arrival-Departure Record I-94 Number, SEVIS ID Number, Certificate of Naturalization Number, Certificate of Citizenship Number, or Unexpired Foreign Passport Number)
- f. Other Information From Immigration Documentation (e.g. Country of Birth, Date of Entry, Employment Authorization Category)

2. From USCIS to CMS. USCIS through SAVE will send the Hub responses that contain data from records provided to VIS and databases VIS accesses. These responses may include the following data elements:

- a. Last Name
- b. First Name
- c. Middle Name
- d. Date of Birth
- e. One or More Immigration Number (e.g. Alien Registration / USCIS Number, Arrival-Departure Record I-94 Number, SEVIS ID Number, Certificate of Naturalization Number, Certificate of Citizenship Number, or Unexpired Foreign Passport Number)
- f. Citizenship or Immigration Data (e.g. immigration class of admission and/or employment authorization)
- g. Sponsorship Data (e.g. name, address, and social security number of Form I-864/I-864EZ sponsors and Form I-864A household members, when applicable)

h. Case Verification Number

D. Projected Starting and Completion Dates of the Matching Program

Effective Date: April 20, 2021

Expiration Date: October 19, 2022 (October 19, 2023 if renewed for 12 months)

V. NOTICE PROCEDURES

The matching notice which CMS will publish in the Federal Register as required by the Privacy Act (5 U.S.C. §552a (e)(12)) will provide constructive notice of the matching program to affected individuals.

The Privacy Act at 5 U.S.C. §552a(o)(1)(D) requires CMAs to specify procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance provided by the Director of OMB pursuant to subsection 552a(v)), to Applicants for and recipients of financial assistance or payments under federal benefit programs. CMS provides actual notice to Applicants and Enrollees that the information they provide when they apply for an eligibility determination may be verified by matching against the records of various federal agencies, including DHS. This notice is provided at the time of application on the OMB-approved HHS-developed single streamlined application or on an HHS-approved alternate application used by an AE. The same application is used by individuals for initial applications and to report changes in circumstances after enrollment. AEs may notify Applicants that they can determine the status of their SAVE verification by visiting SAVE Case Check, which can be accessed through the SAVE public website located at <https://www.uscis.gov/SAVE>.

VI. VERIFICATION PROCEDURES AND OPPORTUNITY TO CONTEST FINDINGS

The Privacy Act at 5 U.S.C. §552a(o)(1)(E) requires that each CMA outline procedures for verifying information produced in the matching program, as required by 5 U.S.C. §552a(p). This requires agencies to independently verify the information produced by a matching program and to provide the affected individual an opportunity to contest the agency's findings, before taking an adverse action against the individual, as a result of the match.

A. Verification Procedures

1. CMS will provide USCIS with the following identifying information about an Applicant or Enrollee for the purpose of obtaining verification from USCIS of the Applicant's or Enrollee's immigration status or naturalized/derived citizenship: date of birth, last name, first name, and middle name, and Alien Registration Number, I-94 number, and/or other identifiers as described in Section IV of this Agreement, as applicable.
2. If USCIS cannot verify immigration status on initial electronic verification (i.e., first step verification), the AE will be prompted to institute additional verification, at which time the AE may submit the case for second step verification or may upload an electronic copy of the Applicant's or Enrollee's immigration document if done in accordance with the rules applicable to the AE for which the request is being made. If USCIS cannot verify immigration status on additional verification, the AE will be prompted to submit the verification request for third level verification. If third level verification is required, the AE

will facilitate the transfer of the Applicant's or Enrollee's immigration documentation to USCIS. The SAVE Program requires copies of immigration documentation in order to conduct third-level verification. The AE must submit such documentation electronically. Submission of paper documentation by mail as an attachment to Form G-845 is no longer a submission option.

3. If an AE is unable to comply with the prompts through the Hub, the AE may implement an approved alternative verification method to verify documents that demonstrate the Applicants' or Enrollee's immigration status. Alternative verification methods should use the AE's independent SAVE access methods to verify immigration and naturalized or derived citizenship status. Alternative access methods that do not use SAVE as an access method to verify immigration and naturalized or derived citizenship status cannot be considered to have received a determination from DHS as to whether the Applicant's information is consistent with information in DHS records. CMS agrees to provide USCIS with written descriptions of any alternative verification procedures, as appropriate, used by AEs.

4. CMS and AEs may not deny an application based on a verification response that fails to verify applicant information with USCIS records unless the AE completes all SAVE prompts returned to the Hub, including submitting the verification request for additional verification or resubmitting the case when prompted by SAVE, or completes an alternate verification procedure.

5. CMS and AEs may not suspend, terminate, reduce, or make a final denial regarding the federal benefit program eligibility of an Applicant or Enrollee under the PPACA based upon a SAVE verification response status, or a response received through an approved alternative method, or take other adverse action against such individual as a result of information produced by the matching program, without first providing the Applicant or Enrollee the opportunity to provide additional information to verify their citizenship or immigration status in accordance with 45 CFR §155.315(f) or 42 CFR §§435.952 and 457.380. See the "additional verification procedures" described in the DHS-USCIS SAVE Program Guide, which procedures are incorporated into this Agreement by reference, including any subsequent amendments or revisions, to the extent that such procedures are consistent with applicable law.

B. Opportunity to Contest Findings

1. CMS and AEs may not suspend, terminate, reduce, or make a final denial regarding federal benefit program eligibility of an Applicant or Enrollee, or take other adverse action against such individual as a result of information produced by this matching program, unless: (A) the individual has received notice from CMS containing a statement of the findings of the immigration status check; and (B) until the subsequent expiration of any notice period provided by such program's law or regulations. Such opportunity to contest may be satisfied by the notice, hearing, and appeal rights governing the federal benefit program if the Applicant has been provided the opportunity to refute any adverse status information as a result of the matching program.

2. Information created by CMS regarding any individual which becomes part of the HIX system of records can be contested by contacting CMS.

3. Because CMS is not the owner of the USCIS records used for verification, information

provided to CMS by USCIS cannot be contested by contacting CMS. An individual seeking to contest the content of USCIS information must contact USCIS or the record's owner. CMS, in its role as operator of the FFE, will provide guidance to the individual concerning how to contest the content of information provided by DHS.

C. Additional Verification and Contest Procedures Applicable to QHPs, APTC and CSRs

1. An Exchange will verify citizenship and immigration status in accordance with 45 CFR §155.315(c). Pursuant to the verification process in 45 CFR §155.315, the Exchange will provide notice to and an opportunity to resolve the inconsistency for the Applicant or Enrollee if there is an inconsistency between the Applicant/Enrollee's attestation and the information provided by DHS/USCIS under this Agreement through the Hub in connection with Eligibility Determinations and Redeterminations for APTC and CSRs. *See also* section 1411(c)(3)(4) of the PPACA. The Applicant/Enrollee will have 90 days from the date of notice of the inconsistency to resolve the inconsistency or to present satisfactory documentary evidence to the agency. 45 CFR §155.315(f).

2. In addition, an Exchange will provide notice of appeals procedures with a notice of Eligibility Determination and Redetermination pursuant to 45 CFR §§155.230 and 155.355. An Applicant or Enrollee will be provided the opportunity to appeal denials of eligibility for APTC and CSRs based upon contested determinations of citizenship or immigration status pursuant to section 1411(f)(1) of the PPACA.

D. Additional Verification and Contest Procedures Applicable to Exemptions

The Exchange will verify certain citizenship and immigration status information provided by an Applicant for a certain type of Exemption with information provided by DHS pursuant to this Agreement in accordance with the process outlined in 45 CFR §§155.615(f) and (g) and 155.620(c). The Exchange will give an affected individual notice of and an opportunity to resolve any inconsistency between the Applicant's attestation and the information obtained from USCIS through the Hub. *See also* Section 1411(e)(3)(4) of the PPACA. In addition, the Exchange will provide notice of appeals procedures in the notice of Eligibility Determination and Redetermination it gives Applicants pursuant to 45 CFR §§ 155.230 and 155.635. An Applicant will be provided the opportunity to appeal denials of eligibility for an Exemption pursuant to section 1411(f)(1) of the PPACA.

E. Additional Verification and Contest Procedures Applicable to Medicaid and CHIP

A state Medicaid or CHIP agency must determine or renew eligibility in accordance with 42 CFR §§435.911, 435.916, 457.340 and 457.343. Medicaid and CHIP agencies will verify certain citizenship and immigration status information provided by an Applicant or beneficiary in accordance with 42 CFR parts 435 or 457. A Medicaid/CHIP Applicant Beneficiary seeking to contest any information used for verification of citizenship or immigration status of an application or Renewal determination that results in an adverse Eligibility Determination may file an appeal with the agency that issued the Eligibility Determination.

F. Additional Verification and Contest Procedures Applicable to BHPs

A BHP will verify an Applicant's or Enrollee's eligibility for a BHP consistent either with the Exchange standards and procedures set forth at 45 CFR §§155.315 and 155.320 or Medicaid standards and procedures set forth at 45 CFR §§ 435.945 through 435.956.

VII. DISPOSITION OF MATCHED RECORDS

These procedures are required by the Privacy Act at 5 U.S.C. §552a(o)(1)(F):

USCIS records are stored and retained in the VIS Master Data File in accordance with the DHS SAVE SORN and retention schedule N1-566-08-7, which was approved by NARA June 5, 2008 and provides a retention period of ten (10) years from the date of completion of the verification (unless the records are part of an ongoing investigation, in which case they may be retained until completion of the investigation).

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 USCIS data received via the Hub.

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

VIII. SECURITY PROCEDURES

As required by the Privacy Act at 5 U.S.C. §552a(o)(1)(G), HHS/CMS and DHS/USCIS agree to the following information security procedures:

A. **General.** Both Parties shall maintain a level of security that is commensurate with the risk and magnitude of harm that could result from the loss, misuse, modification, or inappropriate disclosure of the information contained on the system with the highest appropriate sensitivity level.

B. **Legal Compliance.** Both Parties shall comply with the limitations on use and disclosure, storage, transport, retention, and safeguarding of data under all applicable federal laws, regulations, and agency guidance.

1. CMS and USCIS will comply with applicable OMB circulars and memoranda, including OMB 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 OMB directives including those published subsequent to the effective date of this Agreement.

2. **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 agencies are responsible for oversight and compliance of their contractors and agents.

3. **Incident Reporting, Potential Loss, and Breach Notification.** CMS and USCIS will

comply with OMB reporting guidelines in the event of a loss, potential loss, security incident, or breach of PII (hereafter referred to as “incident”). See OMB M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information” (Jan. 3, 2017), and OMB M-21-02, Fiscal Year 2020-2021 “Guidance on Federal Information Security and Privacy Management Requirements” (Nov. 9, 2020). The Party experiencing the incident will notify the other agency's System Security Contact named in this Agreement within one (1) hour of discovering the incident. If the Party experiencing the incident is unable to speak with the other Party'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:

- USCIS Service Desk: 1-888-220-5228 or e-mail USCIS.ServiceDesk@uscis.dhs.gov;
- CMS IT Service Desk: 1-800-562-1963 or e-mail CMS_IT_Service_Desk@cms.hhs.gov

4. 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 OMB 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 without cost to the other party.

5. 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.

6. Physical Safeguards. Both Parties agree to maintain all automated matching records in a secured computer environment that includes the use of authorized access codes (passwords and/or personal identity verification or PIV) to restrict access and that is otherwise physically safe from access by unauthorized persons at all times. 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. 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. USCIS and CMS will comply with physical security and storage requirement under DHS Sensitive Systems Policy 4300A.

7. Technical Safeguards. Both Parties will process the matched data and any data created by the match 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. The DHS/USCIS personnel will be trained on the new data and process as part of their continued and regular training sessions. 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.

8. Systems personnel will be required to enter personal identification numbers when accessing data on the agencies' systems. Both Parties will strictly limit authorization to these electronic data systems necessary for the authorized user to perform their official duties. Data will be protected in accordance to DHS 4300A, FISMA and NIST security guidance. All data in transit will be encrypted using algorithms that meet the requirements of FIPS 140-3, Security Requirements for Cryptographic Modules, as amended, and implementation guidance. Authorized system users will be identified by login credentials, and individually tracked to safeguard against the unauthorized access and use of the system.

9. 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 solely as provided in this Agreement. Both Parties will comply with these policies and procedures and any subsequent revisions.

10. On-Site Inspections. Each party has the right to monitor the other party's compliance with FISMA requirements for data exchanged under this Agreement, and to audit compliance with this Agreement, if necessary, during the lifetime of this Agreement, or any extension of this Agreement. Each party will provide the other party with any reports and/or documentation relating to such inspections at the other party's request. Each party may request an on-site inspection in addition to requesting reports and/or documentation.

11. Risk Safeguards. CMS will ensure its information systems and data exchanged under this Agreement comply with Acceptable Risk Safeguards. To the extent these documents are revised during the term of this Agreement, CMS will ensure compliance with the revised version.

12. Non-discrimination. Any action required or permitted under this Agreement shall be conducted in a manner that does not discriminate against an individual based upon his or her national origin, race, color, sex, religion, or disability in accordance with Section 705 of the Homeland Security Act of 2002; Section 504 of the Rehabilitation Act of 1973, and agency implementing regulations at 6 CFR Part 15.d.

IX. RECORDS USAGE, DUPLICATION, AND REDISCLOSURE RESTRICTIONS

As required by the Privacy Act at 5 U.S.C. §552a(o)(1)(H), the Parties will comply with the

following limitations on use, duplication, and disclosure of the electronic files and data each Party provides to the other under this Agreement:

A. The Parties will use and disclose the data only for the purposes described in this Agreement or authorized by applicable law, unless the other Party consents to the use or disclosure. The Party requesting permission must specify the following in writing; (1) which data will 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.

B. The Parties will not use the data to extract information concerning individuals therein for any purpose not specified by this Agreement or applicable law.

C. The matching data provided by USCIS under this Agreement will remain the property of USCIS and will be retained by CMS and AEs to be used for internal audits to verify the accuracy of matches and to adjudicate appeals. USCIS matching data will only be destroyed after the matching activity, appeals and audits involving the data have been completed as described under this Matching Program.

D. CMS will restrict access to the results of the data matches maintained in the FFE to the relevant Applicant or Enrollee, application filer, and Authorized Representatives of such persons; as well as to Agents and Brokers who have been authorized by the Applicant and are under agreement with the FFE. CMS shall require compliance with the same or more stringent privacy and security standards as a condition of any contract or agreement with an individual or entity, such as an Agent or Broker, that allows the individual or entity to; (1) gain access from the Exchange to PII submitted to an Exchange or (2) collect, use, or disclose PII gathered directly from Applicants or Enrollees while the individual or entity is performing the functions outlined in the agreement with the Exchange. *See* 45 CFR §155.260, 42 CFR § 431, subpart F, including §§431.301, 431.302, 431.303, 431.305, and 435.945, and 457.1110.

E. Any individual who knowingly and willfully uses or discloses information obtained pursuant to this Agreement in a manner or for a purpose not authorized by Section 1411(g) of the PPACA is potentially subject to the civil penalty provisions of Section 1411(h)(2) of the PPACA, which carries a fine of up to \$25,000 per person or entity per use or disclosure.

F. CMS will not duplicate or re-disclose data provided by USCIS within or outside of CMS, except where described in this Agreement or authorized by applicable law.

X. RECORDS ACCURACY ASSESSMENTS

Pursuant to 5 U.S.C. §552a(o)(1)(J), below is information on assessments made by CMS and USCIS on the accuracy of the records that will be used in the matching program.

USCIS currently estimates that SAVE system accuracy, defined as the number of SAVE initial verification request cases resolved automatically by SAVE divided by the number of initial verification cases that should have been resolved automatically (i.e. number resolved automatically plus number resolved by status verification personnel that should have been resolved automatically), to be 97.5 percent. USCIS continues to undertake various actions to further improve the accuracy of SAVE responses to verification requests. In cases in where SAVE provides an Institute Additional Verification response or an AE or benefit applicant does not agree with the SAVE initial verification response, AEs use an additional verification process that allows USCIS personnel to check all necessary indices and files before providing

the immigration and citizenship information. This process includes procedures for USCIS to alert the relevant immigration record owner of errors it detects so the record owner may take appropriate corrective action.

XI. COMPTROLLER GENERAL ACCESS

Pursuant to 5 U.S.C. § 552(o)(1)(K), the Government Accountability Office (Comptroller General) may have access to all CMS, USCIS, and AE records, as necessary, in order to monitor or verify compliance with this Agreement.

XII. REIMBURSEMENT/FUNDING

Reimbursement for immigration status verifications USCIS performs under this Agreement is addressed under a separate billing agreement. This Agreement is subject to the availability of funds.

XIII. DURATION OF AGREEMENT

A. **Effective Date:** The Effective Date of this Agreement will be April 20, 2021, provided that CMS 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 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)(12).

B. **Term:** The 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 twelve (12) months if CMS and DHS 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.

F. Notwithstanding any other provision in the Agreement, DHS may suspend or terminate this Agreement without prior notice upon a determination by DHS that there has been a breach of system integrity or security by CMS or an AE that cannot be remedied.

XIV. PERSONS TO CONTACT

The USCIS contacts are:

1. Project Coordinator

Jonathan Mills, Chief, SAVE Program
Verification Division MS 2620
United States Citizenship and Immigration Services 131 M Street, NE, Suite 200
Washington, DC 20529-2620
Phone: (202) 306-9874
E-Mail: Jonathan.M.Mills@uscis.dhs.gov

2. Safeguards and Recordkeeping Procedures

Laura Ragan Henry, Chief, Verification Policy
Verification Division MS 2620
United States Citizenship and Immigration Services
131 M Street, NE, Suite 200 Washington, DC 20529-2620
Telephone: (202) 425-2530
E-Mail: Laura.Ragan.Henry@uscis.dhs.gov

Stephen W. Martin, Management & Program Analyst
Verification Policy
Verification Division MS 2620
United States Citizenship and Immigration Services
131 M Street, NE, Suite 200
Washington, DC 20529-2620
Phone: (202) 507-2783
E-Mail: stephen.w.martin@uscis.dhs.gov

3. Privacy Matters

Donald K. Hawkins Privacy Officer
United States Citizenship and Immigration Services
20 Massachusetts Avenue, NW, 5th Floor
Telephone: (202) 272-8404
Email: Donald.K.Hawkins@uscis.dhs.gov

The CMS contacts are:

1. Program Matters

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 Matters

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.Boughn1@cms.hhs.gov

3. Systems and 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 Matters

Barbara Demopulos, Privacy Advisor
Division of Security, Privacy Policy & Governance
Information Security & Privacy Group
Office of Information Technology
Centers for Medicare & Medicaid Services
Location: N1-14-40
7500 Security Boulevard
Baltimore, MD 21244-1850
Telephone: (410) 786-6340
Email: Barbara.demopulos@cms.hhs.gov

XV. 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. § 1346(b)), or pursuant to other Federal statutory authority.
- C. 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.

D. 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.

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

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

XVI. 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 the USCIS and CMS for the purposes described in this Agreement. The parties 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.

XVII. APPROVALS

A. Centers for Medicare & Medicaid Services Program Official

The authorized program official, whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, 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 D. Grant
Deputy Director for Operations
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services

Date _____

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 Shields
Deputy Director
Center for Medicaid and CHIP Services
Centers for Medicare & Medicaid Services

Date _____

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

Date _____

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

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.

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

Date _____

C. U.S. Citizenship and Immigration Services Approving Official

The authorized approving 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.

Amy J. Wheelock, Acting Chief
Verification Division
Immigration Records and Identity Services Directorate
U.S. Citizenship and Immigration Services
Department of Homeland Security

Date _____

D. U.S. Department of Homeland Security Data Integrity Board 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.

Dena Kozanas
Chief Privacy and Freedom of Information Act Officer
Chairperson of the Data Integrity Board
U.S. Department of Homeland Security

Date _____

Attachment 1

Marketplace Computer Matching Programs:
Cost-Benefit Analysis