COMPUTER MATCHING AGREEMENT BETWEEN DEPARTMENT OF HEALTH AND HUMAN SERVICES CENTERS FOR MEDICARE & MEDICAID SERVICES AND STATE BASED ADMINISTERING ENTITIES FOR DETERMINING ELIGIBILITY FOR ENROLLMENT IN APPLICABLE STATE HEALTH SUBSIDY PROGRAMS UNDER THE PATIENT PROTECTION AND AFFORDABLE CARE ACT

Department of Health and Human Services No. 2101 Centers for Medicare & Medicaid Services No. 2021-11 Effective Date: **May 14, 2021 Expiration Date: November 13, 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 Health and Human Services, Centers for Medicare & Medicaid Services (CMS) will disclose certain information to the State Based Administering Entities (AE) to assist them in verifying applicant information as required by the Patient Protection and Affordable Care Act of 2010 (PPACA) in order to make Eligibility Determinations for enrollment in "applicable State health subsidy programs," including exemption from the requirement to maintain Minimum Essential Coverage (MEC) or from the individual responsibility payment.

In accordance with current regulations, State Medicaid and Children's Health Insurance Program (CHIP) agencies shall be the Source Agencies when making Eligibility Determinations via the CMS Data Services Hub (the Hub). To avoid dual enrollment, CMS as the Federally-facilitated Exchange (FFE), and the State Based Exchanges (SBE) shall also serve as the Recipient Agency under this Agreement, with respect to verifying whether an Applicant or Enrollee who has submitted an application to the FFE or an SBE has current eligibility or enrollment in a Medicaid/CHIP program. The responsible component for CMS is the Center for Consumer Information & Insurance Oversight (CCIIO).

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

B. Legal Authorities

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

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

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

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

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

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

C. Definitions

For purposes of this Agreement, the following definitions apply:

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

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

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

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

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

6. "Breach" is defined 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 personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

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

8. "CSR" means cost-sharing reductions for an eligible individual enrolled in a silver level plan through the Exchange or for an individual who is an Alaskan Native/American Indian enrolled in a QHP through the Exchange.

9. "Eligibility determination" means the determination of eligibility for enrollment in an applicable State health subsidy program, or certifications of exemption from the requirement to maintain MEC or the individual shared responsibility payment. The term

"eligibility determination" includes initial assessments and determinations, mid-year and annual redeterminations, and renewals, and any appeal process related to an eligibility determination.

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

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

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

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

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

15. "Personally Identifiable Information" or "PII" is defined by OMB M-17-12 (January 3, 2017), and means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

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

17. "Qualified Health Plan" or "QHP" means an insurance plan under the PPACA that is certified by an Exchange in each state in which it is sold, provides essential health benefits, follows established limits on cost-sharing (like deductibles, copayments, and out-of-pocket maximum amounts), and satisfies other requirements.

18. "Recipient Agency" means any agency, or contractor thereof, receiving records contained in a System of Records from a Source Agency for use in a matching program.

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

20. "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.

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

22. “Source Agency” means any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program.

II. RESPONSIBILITIES OF THE PARTIES

A. CMS Responsibilities:

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

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

3. CMS will develop procedures and conditions through and under which an AE may request information via the Hub from available data sources, which include but arenot limited to CMS, the Internal Revenue Service (IRS), Social Security Administration (SSA), Department of Homeland Security (DHS), Department of Veterans Affairs (VA), Department of Defense (DOD), Peace Corps (PC), Office Personnel Management (OPM), and commercial databases of income and employment, to support eligibility determinations.

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

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

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

B. AE Responsibilities:

1. AE will only request data or data verifications from CMS that are necessary tomake

eligibility determinations as described under Section IV.C.

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

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

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

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

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

III. JUSTIFICATION AND ANTICIPATED RESULTS

A. Cost BenefitAnalysis

In accordance with 5 U.S.C. §552a(u)(4)(A), a cost benefit analysis (CBA) is included as Attachment 1. The CBA covers this and seven other "Marketplace" matching 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 monetary benefits sufficient to offset the costs, because the Marketplace matching programs are not intended to avoid or recover improper payments. The CBA, therefore, does not demonstrate that the matching program is likely to be cost-effective.

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

B. Other Supporting Justifications

Even though the Marketplace matching programs are not demonstrated to be cost-effective, ample justification exists in the CBA sections III (Benefits) and IV (Other Benefits and Mitigating Factors) to

justify DIB approval of the matching programs, including the following:

1. The Marketplace matching programs have resulted in efficient and accurate consumer eligibility determinations and MEC checks, and substantially reduce the administrative burden on CMS and AEs.

2. The matching programs provide a significant benefit to the public by allowing CMS and AEs to quickly and accurately determine consumer eligibility for QHPS and IAPs while minimizing consumer burden.

3. An efficient eligibility and enrollment process contributes to greater numbers of consumers enrolling in Marketplace QHPs, resulting in a reduction of the uninsured population, therefore improving overall health care delivery.

4. Continuing to use the current matching program structure, which is less costly than any alternative structure, is expected to increase the public's trust in the participating agencies as stewards of taxpayer dollars.

C. Specific Estimate of Any Savings

There are no cost savings to conducting the Marketplace matching 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 each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program.

A. System of Records

The CMS System of Records that supports this matching program is the "CMS Health Insurance Exchanges System (HIX)", CMS System No. 09-70-0560, last published in full at 78 Federal Register (Fed. Reg.) 63211 (October 23, 2013), and amended at 83 Fed. Reg. 6591 (February 14, 2018). Routine use 3 of the SOR allows the disclosure under this

agreement.

B. Number of Records Involved

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

C. Specified Data Elements Used in the Match

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

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

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

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

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

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

i. This service is available to all AEs.

b. Verify Lawful Presence (which includes verification of immigration status and naturalized or derived citizenship status).

i. This service is available to all AEs.

c. Verify Annual Income and Family Size (Federal Tax Information).

i. This service is available to all AEs authorized to received Federal Tax Information from the IRS.

d. Verify Current Income from other sources.

i. This service is available to all AEs.

e. Verify Employer-Sponsored Insurance (ESI) MEC.

i. This service is available to all SBEs and BHPs.

f. Verify Non-ESI MEC.

i. Medicaid/CHIP can use this service to verify Medicaid MEC.

ii. SBEs and BHPs can use this service to verify: Medicare, TRICARE, VHA, and Peace Corps MEC.

g. Periodic Eligibility Verification Bulk Service (includes date of death and Medicare MEC).

i. This service will be available to all AEs, but is specifically designed for use by SBEs for periodic checks of current enrollees.

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

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

D. Projected Starting and Completion Dates of the Matching Program

Effective Date – May 14, 2021
Expiration Date – November 13, 2022 (November 13, 2023, if renewed for one year)

V. NOTICE PROCEDURES

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

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

B. At the time of application, AE will provide individual notice (Privacy Act Statement) on the approved streamlined eligibility application regarding the collection, use, and disclosure of the Applicant's PII by the AE; such application shall be either the CMS developed model application (approved under OMB No. 0938-1191) or an alternate state application approved by HHS. The single streamlined application which CMS has developed contains a Privacy Act statement describing the purposes for which the information is intended to be used and the authority which authorizes the collection of the information.

In addition, when an Applicant submits an application for an exemption, depending on whether the SBE will make the eligibility determination for the exemption itself or whether the SBE will utilize the Federally managed service to make the eligibility determination for an exemption, the SBE or CMS will provide individual notice on the exemption application regarding the collection, use and disclosure of the Applicant's PII. The exemption application contains a Privacy Act statement describing the purposes for which the information is intended to be used and the authority which authorizes the collection of the information.

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

VI. VERIFICATION PROCEDURES AND OPPORTUNITY TO CONTEST FINDINGS

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

A. Verification and Opportunity to Contest Findings

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

Information that is provided via the Hub by other data sources, and information that originates with other data sources and is disclosed by CMS through the Hub, cannot be corrected by contacting CMS. Individuals must contact the relevant data source that

provided those records via the Hub in order to correct such records. An individual seeking to contest the content of information that HHS or another data source provided to an Exchange for matching purposes should contact the relevant data source. Under 26 U.S.C. § 7852(e), return information cannot be corrected without filing an amended tax return with the IRS.

B. Contesting Findings

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

1. If the AE is an Exchange, an individual seeking to resolve inconsistencies between attestations and the results of electronic verification for the purposes of completing an eligibility determination should be provided the opportunity to follow the procedures outlined in 45 CFR § 155.315(f). The AE will provide the 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 an inconsistency between an attestation and the result of an electronic verification for the purposes of completing an eligibility determination should be provided the opportunity to follow the procedures outlined in 42 CFR §§ 435.952, 435.956 and 457.380. The AE will provide the 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 Exchange verification procedures at 45 CFR §§ 155.315 and 155.320, or Medicaid verification procedures at 45 CFR § 435.945-956; and must resolve inconsistencies as set forth in paragraphs VI.B.1 and 2 above.

VII. DISPOSITION OF MATCHED ITEMS

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

VIII. SECURITY PROCEDURES

A. Safeguards

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

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

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

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

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

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

3. Technical Safeguards: Both Parties agree that the data exchanged under this Agreement will be processed under the immediate supervision and control of authorized personnel to protect the confidentiality of the data in such a way that unauthorized persons cannot retrieve any such data by means of computer, remote terminal, or other means. AE personnel must enter personal identification numbers

when accessing data on the Party's systems. Both Parties will strictly limit authorization to those electronic data areas necessary for authorized persons to perform his or her official duties.

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

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

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

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

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

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

   b. Establish procedures for secure storage of return information consistently

maintaining two barriers of protection to prevent unauthorized access to the information, including when in transit, in accordance with Publication 1075, section 4.0.

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

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

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

f. Prior to initial receipt of return information, have an IRS approved Safeguard Security Report (SSR). Each AE's Head of Agency must certify the SSR fully describes the procedures established for ensuring the confidentiality of return information, addresses all outstanding actions identified by the Office of Safeguards from a prior year's SSR submission; accurately and completely reflects the current physical and logical environment for the receipt, storage, processing and transmission of FTI; accurately reflects the security controls in place to protect the FTI in accordance with Publication 1075 and the commitment to assist the Office of Safeguards in the joint effort of protecting the confidentiality of FTI; report all data incidents involving return information to the Office of Safeguards and Treasury Inspector General for Tax Administration (TIGTA) timely and to cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident; support the Office of Safeguards' on-site review to assess compliance with Publication 1075 requirements by means of manual and automated compliance and vulnerability assessment testing, including coordination with information technology (IT) divisions to secure pre-approval, if needed, for automated system scanning and to support timely mitigation of identified risk to return information in a Corrective Action Plan (CAP) for as long as return information is received or retained. SSR will be transmitted in

electronic format and on the template provided by Office of Safeguards using an IRS approved encryption method in accordance with Publication 1075, Section 7.0.

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

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

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

j. Report suspected unauthorized inspection or disclosure of return information within 24 hours of discovery to the appropriate Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA), and to the IRS Office of Safeguards in accordance with as specified in Publication 1075, section 10.0.

k. Allow IRS to conduct periodic safeguard reviews of the AE to assess whether security and confidentiality of Return Information is maintained consistent with the safeguarding protocols described in Publication 1075. Periodic safeguard reviews will involve the inspection of AE facilities and contractor facilities where FTI is maintained; the testing of technical controls for computer systems storing, processing or transmitting FTI; review of AE recordkeeping and policies and interviews of AE employees and contractor employees as needed, to verify the use of FTI and assess the adequacy of procedures established to protect FTI.

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

property of the IRS; that they constitute IRS official agency records; that any request for the release of IRS records is subject to disclosure restrictions under Federal law and IRS rules and regulations and that any requestor seeking access to IRS records should be referred to the Federal Freedom of Information Act (FOIA) statute. Federal agencies in receipt of FOIA requests for safeguards documents must forward them to IRS for reply.

E. Incident Handling and Reporting

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

   a. Identify Incidents involving matching data that constitute PII.

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

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

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

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

   a. SBE and BHP report a Security Incident or Breach of PII to HIX.incidents@cms.hhs.gov within one hour of discovery of the incident by completing incident form. That e-mail will inform the appropriate designated CMS staff and the following affected Federal agency data sources, i.e., Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management, and Veterans Health Administration. If an SBE suspects a security incident may warrant a disconnection of the system-to-system connection to CMS and/or the Hub due to the severity of the incident and potential threat to CMS and other Federal systems, the SBE must immediately contact the CMS IT Service Desk at (410)

786-2580 or via email at CMS_IT_Service_Desk@cms.hhs.gov.

b. SBE and BHP report any incident involving FTI to the Internal Revenue Service (IRS) Office of Safeguards by e-mail to safeguardreports@irs.gov. Additionally, SBE must telephone the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-589-3718. SBE should not wait until after their own internal investigation has been conducted to report an incident to CMS, TIGTA, and the IRS.

Medicaid and CHIP agencies operating in a state in which the FFE operates will report a loss, potential loss, Security Incident or Breach of PII to the CMS IT Service Desk at (410) 786-2580. CMS will then notify the following affected Federal agency data sources, i.e., Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management, and Veterans Health Administration. State Medicaid and CHIP agencies are also responsible for reporting any suspected or confirmed incident involving FTI directly to the office of the appropriate Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards within 24 hours of discovery of any potential Breach, loss, or misuse of return information. Contact information is contained in § 10.1, IRS Publication 1075, http://www.irs.gov/pub/irs-pdf/p1075.pdf.

c. A Medicaid and/or a CHIP agency, when operating as an AE performing Exchange functions under a SBE, reports to HIX.Incidents@cms.hhs.gov. Affected Federal agency data sources, i.e., Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management, or Veterans Health Administration receive notifications from the HIX mailbox. Additionally, the Medicaid/CHIP agency shall contact the office of the appropriate Special Agent-in-Charge, TIGTA, and the IRS Office of Safeguards within 24 hours of discovery of any potential Breach, loss, or misuse of FTI. Contact information is contained in Section 10.1, IRS Publication 1075, http://www.irs.gov/pub/irs-pdf/p1075.pdf. The Medicaid and/or CHIP agency shall handle and report incidents in accordance with the organization's documented incident handling and breach notification procedures in accordance with 42 CFR §§ 431.300-431.306, and 435.945.

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

F. Administering Entity Opt Out for Receiving FTI

Notwithstanding the requirements related to FTI in this Section VIII or in any section of this Agreement, if an AE that is a Party to this Agreement opts out of receiving FTI provided by the IRS in connection with eligibility determinations and does not receive such FTI, that AE shall not be bound by any of this Agreement's terms governing the receipt,

use, disclosure or safeguarding of FTI. Should that AE revise its position at any time during the term of this Agreement and so notify CMS of its intent to receive FTI, the AE must comply with the terms of this Agreement as it relates to the safeguarding of FTI as of the date of such notice; provided, however, that no FTI will be disclosed to the AE without an IRS approved Safeguard Security Report.

IX. RECORDS USAGE, DUPLICATION, AND REDISCLOSURE RESTRICTIONS

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

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

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

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

1. The AE will restrict access to the matching data to Applicants, Enrollees, Application Filers, and Authorized Representatives of such persons. AE shall execute with each individual or entity such as agents or brokers that (1) gain access from the AE to PII submitted to an Exchange or (2) collect, use, or disclose PII gathered directly from Applicants, or Enrollees while that individual or entity is performing the functions outlined in its agreement with the AE, a written contract or agreement that includes (1) a provision describing the functions to be performed by the individual or entity and strictly limiting the use and disclosure of PII to those functions; (2) a provision(s) binding the individual or entity to comply with the same privacy and security standards and obligations that are made applicable to the PII under this Agreement, as appropriate, and specifically listing or incorporating those privacy and security standards and obligations; (3) a provision requiring the individual or entity to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls; (4) a provision requiring the individual or entity to inform the AE of any change in its administrative, technical, or operational environments defined as material within the contract; (5) a provision that requires the individual or entity to bind any downstream entities to the same privacy and security standards and obligations to which the individual or entity has agreed in its contract or agreement with the AE. Medicaid and Children's Health Insurance Program (CHIP) agencies also must assure that it will provide safeguards which restrict the use or disclosure of information concerning Applicants and recipients to purposes directly connected with the administration of the Medicaid and CHIP programs. This includes the disclosure of electronic data used to make an

Eligibility Determination. 42 CFR § 431, subpart F, including §§ 431.301, 431.302, 431.303, 431.305, and 435.945, and 42 CFR § 457.1110.

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

X. RECORDS ACCURACY ASSESSMENTS

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

XI. COMPTROLLER GENERAL ACCESS

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

XII. REIMBURSEMENT/FUNDING

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

XIII. DURATION OF AGREEMENT, MODIFICATION, AND TERMINATION

A. The Effective Date of this Agreement is May 14, 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. The AE and CMS 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 AE certify the following to the HHS DIB:

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

C. 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 date shall be effective ninety (90) days after the date of the notice or at a later date specified in the notice provided this date does not exceed the approved duration for the agreement. A copy of this notification should be submitted to the Secretary, HHS DIB.

XIV. PERSONS TO CONTACT

A. CMS

1. Programmatic Issues between CMS and the Federal Hub Data Partners:

Terence Kane
Director, Division of Eligibility Verifications
Marketplace Eligibility and Enrollment Group
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services7501 Wisconsin Avenue
Bethesda, MD 20814
Telephone: (301) 492-4449
Fax: (443) 821- 4263
Email: Terence.Kane@cms.hhs.gov

2. State Based Exchange Programmatic Issues:

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

Robert Yates
State Operations Division
State Marketplace and Insurance Programs Group
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services
7501 Wisconsin Avenue
Bethesda, MD 20814
Telephone: 301-492-5151
E-mail: Robert.Yates@cms.hhs.gov

3. Medicaid/CHIP Programmatic Issues:

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

4. Medicaid/CHIP System issues:

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
E-mail: Julie.Boughn1@cms.hhs.gov

5. Privacy Policy and Agreement Issues:

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

6. Marketplace Privacy and Security Issues:

Marc Richardson
Acting Director
Marketplace Information Technology Group
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services
7500 Security Boulevard Mail Stop: N1-26-05
Baltimore, MD 21244-1850
Telephone: (410) 786-0016

E-mail: March.Richardson@cms.hhs.gov

B. The contact person for the AE can be found on the AE's signaturepage.

XV. APPROVALS

A. Centers for Medicare & Medicaid Services Program Official

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

Approved by (Signature of Authorized CMS Program Official)

Jeffrey Grant -S Digitally signed by Jeffrey Grant -S
Date: 2020.12.01 18:39:12 -05'00'

Jeffrey Grant **Date:**
Deputy Director for Operations
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services

B. Centers for Medicare & Medicaid Services Program Official

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

Approved by (Signature of Authorized CMS Program Official)

Karen M Shields -S Digitally signed by Karen M. Shields -S
Date: 2020.12.11 08:20:07 -05'00'

Karen Shields **Date:**
Deputy Director
Center for Medicaid and CHIP Services
Centers for Medicare & Medicaid Services

C. Centers for Medicare & Medicaid Services Approving Official

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

Approved By (Signature of Authorized CMS Approving Official)

Michael E Pagels -S Digitally signed by Michael E. Pagels -S
Date: 2020.12.1 09:05:19 -05'00'

Michael Pagels **Date:**
Director

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

D. 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 his respective organization to the terms of this Agreement.

Approved By (Signature of Authorized HHS DIB Official)

James B. Duncan -S Digitally signed by James B. Duncan -S
Date: 2021.03.02 16:42:32 -05'00'

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

E. Participating AE Program Official

1. AE Model

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

The AE under this Agreement is:

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

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

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

The authorized program official, who should be designated by the AE, and whose signature appears below, accepts and expressly agrees to the terms and conditions expressed herein, confirms that no verbal agreements of any kind shall be binding or recognized, and hereby commits his/her respective organization to the terms of this Agreement. Each AE will sign a separate copy of this Agreement.

Approved by (Signature of Authorized AE Official)

Name **Date:**
Title
Organization

Attachment 1: Master Cost Benefit Analysis

Attachment 2: Guidance Regarding Identity Proofing for the Marketplace, Medicaid, and CHIP, and the Disclosure of Certain Data Obtained through the Data Services Hub

ATTACHMENT 2

Guidance Regarding Identity Proofing for the Marketplace, Medicaid, and CHIP, and the Disclosure of Certain Data Obtained through the Data Services Hub
June 11, 2013

We encourage states that would like to discuss the impact of these changes on design, as well as state-specific implementation approaches, to contact their CCIIO State Officer or CMCS State Operations and Technical Assistance (SOTA) lead, as applicable. We also note that we will continue to work with our Federal and state partners to explore additional solutions for future years.

Q1: What is identity proofing? Why is it necessary?

A1: In the context of the Marketplace, Medicaid, and CHIP, identity proofing refers to a process through which the Marketplace, state Medicaid agency, or state CHIP agency obtains a level of assurance regarding an individual's identity that is sufficient to allow access to electronic systems that include sensitive state and Federal data. Identity proofing is used throughout the public and private sector to ensure the privacy of personal information, such that only the appropriate individuals have access to data to which access is restricted. In this context, a robust identity proofing process is a key piece of the comprehensive privacy and security framework that is needed when providing interactive access to an eligibility process that includes sensitive Federal and state data. Once identity proofing has been completed, the individual who has been proofed may consent to the use and disclosure of trusted data necessary for making an eligibility determination, including data from Federal agencies. For the Marketplace, Medicaid, and CHIP, identity proofing will rely on an electronic process to the maximum extent possible, and may also include a combination of paper-based and in-person approaches. We also note that identity proofing as described here is distinct from the citizenship and identity verification process specified in the Deficit Reduction Act of 2005 (Pub. L. No. 109-171), although we have taken steps to ensure operational alignment where possible to ease state implementation.

Q2: Who must be identity proofed as part of an online or telephonic application for enrollment in a qualified health plan (QHP) through the Marketplace in the individual market, advance payments of the premium tax credit, cost-sharing reductions, Medicaid and CHIP?

A2: In order to submit an online or telephonic application for enrollment in a qualified health plan (QHP) through the Marketplace in the individual market, advance payments of the premium tax credit, cost-sharing reductions, Medicaid and CHIP, the adult[1] application filer must complete identity proofing sufficient to provide CMS assurance level 2. An authorized representative for an applicant who is identified on the application must complete identity proofing sufficient to provide CMS assurance level 2. Please see question 11 regarding the process for application filers who are unable to complete electronic proofing.

We will provide future guidance regarding the applicability of identity proofing to a certified application counselor, in-person assister, agent, broker, or Navigator who is identified on the application as assisting the application filer, as well as to an employee or contractor of a Marketplace, state Medicaid agency, or state CHIP agency who is viewing personally identifiable information from applications and Federal data sources.

[1] If the application filer is an emancipated minor, he or she will also need to complete identity proofing.

Q3: Who must complete identity proofing as part of an online or telephonic application for SHOP?

A3: In order to submit an online or telephonic application for SHOP, employees, as well as primary and secondary employer contacts, will need to complete identity proofing sufficient to provide CMS assurance level 2.

Q4: When must identity proofing occur?

A4: The Federally-facilitated Marketplace (FFM) will be inserting the identity proofing process before the start of the online application. An application filer must complete identity proofing prior to the disclosure of any information obtained through the Hub to the application filer. We will provide future guidance regarding the applicability of identity proofing to a certified application counselor, in-person assister, agent, broker, or Navigator who is identified on the application as assisting the application filer.

Q5: What is necessary to achieve levels of assurance 1 and 2?

A5: See the below chart for information on the processes that the FFM will use to achieve assurance levels 1 and 2. A state-based Marketplace, state Medicaid agency, or state CHIP agency may utilize different processes, to the extent that they comply with privacy and security standards.

Level of Assurance	Process
Level 1	• *Remote:* Confirmation via e-mailed link
Level 2	• *Remote:* Collection of core attributes, including name, date of birth, SSN (optional), address, phone number, and e-mail address; validation of core attributes with trusted data source; collection and validation of responses to knowledge-based questions for a share of the population. • *Delegated:* Remote or in-person proofing completed by a trusted entity

Q6: What services will CMS provide to support identity proofing?

A6: CMS will provide a remote identity proofing (RIDP) service that is available to Marketplaces, state Medicaid agencies, and state CHIP agencies through the Data Services Hub (Hub) and supports CMS assurance levels 2 and 3. This service will accept core data elements from the requesting entity, provide identity proofing questions (also known as "out-of-wallet" questions) as applicable, validate the core data elements and responses to identity proofing questions, and provide a response as to whether proofing is complete, or whether additional proofing is necessary. If additional proofing is necessary, the requesting entity will refer the individual who is being proofed to a call center that is associated with the RIDP service, which will provide the individual with an additional opportunity to complete proofing. The RIDP service will notify the requesting entity regarding the outcome of this interaction. Please see question 11 regarding the process for application filers who are unable to complete electronic proofing, which will be managed by the Marketplace, state Medicaid agency, or state CHIP agency that is accepting the application. CMS will also provide a multi-factor authentication (MFA) service that is available to Marketplaces, state Medicaid agencies, and state CHIP agencies through the hub.

Q7: Will Federal tax information (FTI) obtained from the IRS via the data services hub, data regarding income from title II benefits obtained from SSA via the data services hub, or the number of quarters of coverage obtained from SSA via the data services hub[2] be disclosed to an application filer, an applicant, or an individual who is identified on the application as assisting
The application filer (agent, broker, certified application counselor, in-person assister, or Navigator) through the application process?

A7: No. In order to reduce the amount of identity proofing needed during the application process, Federal tax information, data regarding income from title II benefits obtained from SSA via the hub, and the number of quarters of coverage obtained from SSA via the hub will be disclosed only to the requesting Marketplace, state Medicaid agency, or state CHIP agency, and used by those entities in the eligibility process. The single, streamlined application will not enable the disclosure of FTI, data regarding income from title II benefits obtained from SSA via the hub, and the number of quarters of coverage obtained from SSA via the hub (for example, through pre-population of the application), and a receiving entity may not disclose it on an eligibility notice or in response to a customer service inquiry. FTI, data regarding income from title II benefits obtained from SSA via the hub, and the number of quarters of coverage obtained from SSA via the hub may be used internally by the Marketplace, state Medicaid agency, and state CHIP agency for the purposes of conducting verifications and determining eligibility for enrollment in a QHP through the Marketplace and for insurance affordability programs as applicable, and must be safeguarded in accordance with applicable regulations and IRS publication 1075 (for FTI). This change has been made to ensure adherence with Federal law, avoid significant consumer experience challenges associated with additional identity proofing for application filers, as well as for other adults in certain circumstances, and to avoid the need to make changes to systems design to facilitate this level of identity proofing.

Changes to the Application

Accordingly, the model single, streamlined application and any state-developed alternative application will not display FTI or data regarding income from title II benefits obtained from SSA via the hub. During the "expedited" income component of the application, the model application for 2014 includes an option for an application filer to attest that his or her projected annual household income for 2014 will be the same as his or her FTI and data regarding income from title II benefits obtained from SSA via the hub (without viewing the IRS and SSA data within the application) or to provide another figure. If an application filer attests that the data on file is an accurate representation of his or her projected annual household income for 2014, the FFM will utilize this attestation for the eligibility determination, and not allow the application filer to view the underlying FTI or data regarding income from title II benefits obtained from SSA via the hub in his or her electronic account, and may not include it on his or her eligibility notice. We note that prior versions of the model single, streamlined application were designed to display FTI and data regarding income from title II benefits obtained from SSA via the Hub. Unfortunately, this disclosure is not possible without additional proofing. The FFM will also not display the number of quarters of coverage obtained from SSA via the hub in the application, electronic account, or eligibility notice. The non-disclosure of quarters of coverage obtained from SSA via the hub does not represent a change from prior drafts of the model application.

[2] Certain states require that an applicant who is a lawful permanent resident have 40 quarters of coverage or more in order to be eligible for Medicaid in that state. These quarters of coverage can be earned by the applicant themselves, a spouse or former spouse of the applicant, if earned when married to the applicant, or a parent of the applicant, if earned while the applicant was under age 18.

Customer Service Inquiries

If an application filer contacts the Marketplace, state Medicaid agency, or state CHIP agency and requests the FTI, data regarding income from title II benefits obtained from SSA via the hub, or the number of quarters of coverage obtained from SSA via the hub used in processing his or her application, the Marketplace, state Medicaid agency, or state CHIP agency will provide the application filer with information on how to move forward to resolve any open verification issue, and may not provide the underlying data. If the applicant is still interested in obtaining the underlying FTI, data regarding income from title II benefits obtained from SSA via the hub, or the number of quarters of coverage obtained from SSA via the hub used in processing his or her application, the Marketplace, state Medicaid agency or state CHIP agency will be able to provide instructions to the applicant on how to locate the data in tax and Social Security benefit documents they already have or how to interact directly with IRS or SSA.

Unresolved Income Inconsistencies for Advance Payments of the Premium Tax Credit and Cost-Sharing Reductions

45 CFR 155.320(c)(3)(vi)(E) specifies that if the Marketplace is unable to verify projected annual household income at the conclusion of the inconsistency period, it will determine eligibility based on FTI and income from title II benefits obtained from SSA via the hub. In this situation, the Marketplace notice to the application filer will include the resulting eligibility determination, including the maximum amount of the advance payment of the premium tax credit (if applicable), and may not include the underlying data. The Marketplace may explain in the notice to the application filer that the resulting determination is based on data from the Internal Revenue Service and the Social Security Administration.

Eligibility Appeals

If an individual appeals his or her eligibility determination and needs access to FTI, the Marketplace, state Medicaid agency, or state CHIP agency will collect a handwritten signature (either an original or a copy) from the adult application filer to authorize the disclosure. If an application includes more than one tax household, or if the individual needs access to data regarding income from title II benefits obtained from SSA via the hub or the number of quarters of coverage obtained from SSA via the hub, the Marketplace, state Medicaid agency, or state CHIP agency will collect handwritten signatures from every adult listed on the application to authorize the disclosure. These signatures can be mailed or uploaded to the Marketplace, state Medicaid agency, or state CHIP agency, and the Marketplace, state Medicaid agency, or state CHIP agency may also elect to receive them via facsimile. We are working with our Federal partners to develop appropriate authorizing language to pair with the signature or signatures, and will share this with states in the future.

Annual Redetermination

We intend to address the treatment of FTI and data regarding income from title II benefits obtained from SSA via the Hub with respect to pre-populated redetermination notices in future guidance.

Failure to Reconcile

Regulations at 45 CFR 155.305(f)(4) provide that APTC will not be provided when the IRS notifies the Marketplace as part of the income verification process for eligibility determinations for 2015 and beyond that APTC was provided on behalf of the tax filer or his or her spouse for a year for which tax data would be utilized for verification of household income and family size, and the tax filer or his or her spouse did not comply with the requirement to file an income tax return for that year. We are working with IRS to ensure that this can be implemented within the constraints on disclosure, and expect that the responsibility of the Marketplace in such a situation will be to notify the application filer to contact the IRS to get information regarding the issue and how to resolve it. We also note that this situation will not occur until the open enrollment period that begins on October 15, 2015.

Data that May be Disclosed

We note that any information provided on an application by an application filer may be displayed as part of the application, eligibility notice, and electronic account. Further, the following data elements that are calculated by the Marketplace, state Medicaid agency, or state CHIP agency are based on multiple sources of data and may be disclosed as part of the eligibility and enrollment process: income and household size as a percentage of the Federal poverty level; the maximum amount of advance payments of the premium tax credit (APTC); and the actual amount of APTC elected by a tax filer during the plan selection process and applied for a given time period.

Q8: Can current income data obtained from Equifax Workforce Solutions via the data services hub be disclosed to an application filer, an applicant, or an individual who is identified on the application as assisting the application filer (agent, broker, certified application counselor, in- person assister, or Navigator) through the application process?

A8: Current income data for an adult obtained from Equifax Workforce Solutions via the data services hub may be disclosed only to the adult himself or herself, to his or her authorized representative, or to any individual identified on the application as assisting the adult (agent, broker, certified application counselor, in-person assister, or Navigator), provided that the adult completes identity proofing sufficient to provide CMS assurance level 2, and any individual identified on the application as assisting the adult completes identity that provides a sufficient level of assurance. Current income data for a minor child obtained from Equifax Workforce Solutions via the data services hub may be disclosed to the legal guardian of the minor child, provided that the legal guardian completes identity proofing sufficient to provide CMS assurance level 2.

If an application filer contacts the Marketplace, state Medicaid agency, or state CHIP agency and requests the data obtained from Equifax Workforce Solutions via the data services hub used in processing his or her application, the Marketplace, state Medicaid agency, or state CHIP agency will provide the application filer with instructions on how to submit information to resolve any open verification issue. The Marketplace, state Medicaid agency, and state CHIP agency will also be able to direct such an individual to Equifax to obtain the source information if necessary.

If an individual appeals his or her eligibility determination and needs access to the data obtained from Equifax Workforce Solutions via the hub, the Marketplace, state Medicaid agency, or state CHIP agency will collect a physical signature (either an original or a copy) from every adult whose data is needed. These signatures can be mailed or uploaded to the Marketplace, state Medicaid agency, or state CHIP agency, and the Marketplace, state Medicaid agency, or state CHIP agency may also elect to receive them via facsimile.

We intend to address the treatment of current income data obtained from Equifax Workforce Solutions via the Hub with respect to pre-populated redetermination notices in future guidance.

Q9: Is Social Security number (SSN) required for the remote identity proofing (RIDP) service?

A9: No. SSN will greatly improve the ability of the RIDP process to provide a sufficient level of assurance, but is not required.

Q10: How does identity proofing affect paper applications?

A10: The identity proofing process described in this set of questions and answers is designed to support the online and telephonic application processes, which will provide immediate feedback based on information contained in Federal data sources. For a paper application, the adult application filer will sign his or her name under penalty of perjury, which is sufficient to enable the Marketplace, state Medicaid agency, or state CHIP agency to adjudicate the application. If an individual who submitted a paper application then wants to move into an electronic process (e.g. to conduct QHP selection online), he or she will need to complete the identity proofing process described in this set of questions and answers.

Q11: What if an individual who needs to complete identity proofing cannot complete the electronic proofing process?

A11: In order to ensure the security of the electronic process, an individual who cannot complete the electronic proofing process will need to submit satisfactory documentation to the Marketplace, state Medicaid agency, or state CHIP agency in order to proceed electronically.
Upon receipt of satisfactory documentation, the Marketplace, state Medicaid agency, or state CHIP agency will upgrade the individual to CMS assurance level 2.

First, an individual can submit a copy of one of the following documents to the Marketplace, state Medicaid agency, or state CHIP agency, provided that such document has either a photograph of the individual or other identifying information of the individual such as name, age, sex, race, height, weight, eye color, or address. Submission can occur through mail or via an electronic upload process.

- Driver's license issued by state or territory
- School identification card
- Voter registration card
- U.S. military card or draft record
- Identification card issued by the Federal, state, or local government, including a U.S. passport
- Military dependent's identification card
- Native American Tribal document
- U.S. Coast Guard Merchant Mariner card

If an individual cannot provide a copy of one of these documents, he or she can also submit two of the following documents that corroborate one another: a birth certificate, Social Security card, marriage certificate, divorce decree, employer identification card, high school or college diploma (including high school equivalency diplomas), and/or property deed or title. A Marketplace, state Medicaid agency, or state CHIP agency may accept additional documents, provided that these documents are described in the Marketplace/agency's security artifacts. The Marketplace, state Medicaid agency, and state CHIP agency should clearly explain to applicants that they should not submit original documents, and should be able to answer questions regarding acceptable documentation and the identity proofing process.

Further, if one of the above documents or combination of documents has been accepted by another state agency, the Marketplace, State Medicaid agency, or State CHIP agency may use this as the basis to upgrade an account to CMS assurance level 2.

Lastly, we also note that an individual who submits a paper application and does not seek electronic access to the eligibility process will not need to provide the documentation for identity proofing purposes.

Q12: Can in-person proofing be substituted for electronic proofing?

A12: A Marketplace, state Medicaid agency, or state CHIP agency may choose to allow in- person proofing when an individual is filing an application in person, although it may not require in-person proofing. In-person proofing for CMS assurance level 2 involves the presentation of a document or documents in accordance with the standards outlined in question 11.

Q13: If identity proofing is successful, does a Marketplace, state Medicaid agency, or state CHIP agency need to repeat it at any point in the future?

A13: We have not yet determined which events would trigger reproofing.

Q14: Can an individual still complete an online or telephonic application if he or she is unable to complete the electronic proofing process?

A14: Yes, such an individual can complete an electronic application that is structured to not provide any real-time feedback (e.g. no interactive SSN validation process, no income verification, no eligibility results). Eligibility results may be provided once proofing is completed through the alternate process.

Technical Questions

Q15: Does the remote identity proofing (RIDP) service have any prevention/detection controls to prevent extensive verification performed for the same information/individual?

A15: Yes. There are a number of fraud detection capabilities through the RIDP service which help determine the level of confidence (e.g., behavior of transaction, IP address blacklists, SSN fraud lists, etc.). CMS will select settings that limit the number of attempts that can be made, the duration in which a person must answer a question and the number of times data can be repeated or presented.

Q16: Does the remote identity proofing (RIDP) service provide a score that will helpthe requesting entity determine the level of confidence with the verification? If not, how is the level of confidence determined? And, will the confidence rating be returned back?

A16: The RIDP service will return whether an individual passed or failed the RIDP process, and will not provide a score. The pass/fail assessment is based upon a confidence matrix which is maintained by CMS.

Q17: Can states use the remote identity proofing (RIDP) service and/or the proofing results obtained through the service for SNAP, TANF and other programs?

A17: The RIDP service can only be initiated for the purposes of identity proofing related to eligibility for enrollment in a QHP through the Marketplace (including through the SHOP), Medicaid, and CHIP or eligibility for an exemption from the shared responsibility payment. However, other programs could use the identity proofing results that were obtained through the RIDP service.

Q18: What are the inputs and outputs for the remote identity proofing (RIDP) service?

A18: Please refer to the RIDP and MFA BSDs available through Centrasite. (DSH_RD_BSD_Remote_ID_Proofing(1).docx and DSH_RD_BSD_MFAUsrMgtAuth.doc, respectively)

Q19: When will the Web Services Description Language (WSDL) for the remote identity proofing (RIDP) service be available?

A19: The service specification for the RIDP service, including the WSDL, is available through Centrasite.

Q20: When will the remote identity proofing (RIDP) service be available for testing?

A20: The RIDP service was made available as part of the wave testing process in March. The MFA service will likely not be available for testing until June.

Q21: Can a Marketplace, state Medicaid agency, or state CHIP agency choose specific identity proofing questions within the remote identity proofing (RIDP) service?

A21: The identity proofing questions available through the RIDP service will be standardized.

Q22: Do any individuals need to be proofed at assurance level 4? Is a hard token mandatory for this level of assurance?

A22: Level 4 is primarily for those with system level or root access to systems and databases. A hard token is required to achieve this level of assurance. CMS suggests that states explore various vendor options as there are several cost-effective solutions in this area.

Q23: Have the identity proofing questions been subject to any Federal focus group reviews to ensure the questions are appropriate and easy to understand?

A23: The vendor providing services to CMS conducts regular consumer studies regarding their question to ensure they are clear and easily understood. CMS is evaluating additional targeted consumer testing and will also be monitoring the implementation of identity proofing and maintaining the capability to make adjustments as needed.

Q24: Is the remote identity proofing (RIDP) service available in Spanish?

A24: Yes, the RIDP service will be available in Spanish.