

## MAC Binder Section 1 – Letters from CMS Part B

Table of Contents with Document Summary

Located online at <http://chfs.ky.gov/dms/mac.htm>

---

### **12-CMS-CMA Agreement 2016-032416:**

Computer Matching Agreement No. 2016-11: The Department of Health and Human Service  
No. 1601 Effective April 2, 2016-October 2, 2017

**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**

**Computer Matching Agreement No. 2016-11  
The Department of Health and Human Services No. 1601**

**Effective Date – April 2, 2016  
Expiration Date – October 2, 2017**

**I. PURPOSE, LEGAL AUTHORITIES, AND DEFINITIONS**

**A. Purpose**

This Computer Matching and Privacy Protection Act (CMPPA) Agreement (Agreement) is required by the Privacy Act of 1974, as amended. This Agreement by and between the Centers for Medicare & Medicaid Services (CMS) and the State-based Administering Entities (AEs) establishes the terms, conditions, safeguards, and procedures under which CMS will disclose certain information to the AEs in accordance with the Patient Protection and Affordable Care Act of 2010 (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act (Public Law 111-152), which are referred to collectively as the Affordable Care Act (ACA), amendments to the Social Security Act made by the ACA, and the implementing regulations. The AEs, which are state entities, will use the data accessed through the Federal Data Services Hub (Hub), to make Eligibility Determinations for enrollment in “applicable State health subsidy programs” (Section 1414(e) of the ACA), including exemption from the requirement to maintain Minimum Essential Coverage or from the individual responsibility payment. All AEs that are connecting to the Federal Data Services Hub or that receive data under this matching program must sign this Computer Matching Agreement.

The terms and conditions of this Agreement will be carried out by authorized officers, employees, and contractors of CMS and AEs. For each State agency signatory to this Agreement, CMS and the relevant AEs are each a “Party” and collectively “the Parties.” In accordance with the CMPPA, CMS shall be the Source Agency and the participating AE shall be the Recipient Agency under this Agreement with respect to information that AEs will receive via the Data Services Hub. In accordance with the CMPPA, State Medicaid/CHIP agencies shall also be the Source Agencies and CMS (as the Federally-facilitated

Marketplace (FFM)), State-based Marketplaces (SBMs) and Basic Health Plans (BHPs) shall be the Recipient Agency under this Agreement with respect to verifying whether an Applicant or Enrollee who has submitted an application to the FFM or an SBM has current eligibility or enrollment in a Medicaid/CHIP program.

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

## B. Legal Authorities

This Agreement is executed in compliance with the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the CMPPA, and the regulations and guidance promulgated thereunder. The following statutes provide legal authority for the disclosures under this Agreement:

1. 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) as amended by the Health Care and Education Reconciliation Act (Public Law 111-152) referred to collectively as the Affordable Care Act (ACA), and implementing regulations at 42 CFR Parts 431, 435, 457, and 45 CFR Parts 155-157.
2. 45 C.F.R. § 155.260 establishes privacy and security requirements for the Marketplaces and for "Non-Exchange Entities," as defined at 45 C.F.R. 155.260(b)(1), to which AEs must adhere.
3. 45 C.F.R. § 155.285(a) establishes standards for imposition of civil money penalties by HHS on any person, including an AE, who knowingly and willfully uses or discloses information in violation of Section 1411(g) of the ACA or 45 C.F.R. § 155.260, or submits false information on a Marketplace application in violation of Section 1411(h) of the ACA.
4. The Privacy Act, 5 U.S.C. § 552a(b)(3), authorizes a Federal agency to disclose information about an individual that is maintained by an agency in an agency system of records, without the prior written consent of the individual, when such disclosure is pursuant to a routine use. There are existing routine uses in the pertinent CMS systems of records for the purpose of making Eligibility Determinations where the disclosure of applicant information to an AE and to non-governmental entities such as an Application Filer is authorized.
5. Section 1943(b) of the Social Security Act (as added by Section 2201 of the ACA) requires Medicaid and CHIP agencies to utilize the same streamlined enrollment system and secure electronic interface established under Section 1413 of the ACA to verify information, including citizenship and satisfactory immigration status, needed to make an Eligibility Determination and facilitate a streamlined eligibility and enrollment system among all Marketplaces, Basic Health Programs, Medicaid and CHIP programs.
6. 45 C.F.R. §§ 155.302 and 155.305 require that a Marketplace determine or assess individual eligibility for Medicaid/CHIP in certain circumstances and ensure that those individuals are enrolled in Medicaid/CHIP coverage.

7. Sections 1311(d)(4)(H) and 1411 of the ACA and implementing regulations adopted by the Secretary of HHS provide for the determination of eligibility for individual responsibility exemptions.
8. Section 1411(a) of the ACA requires the Secretary to establish a program for determining eligibility for enrollment in a qualified health plan (QHP) through the Marketplace, advance payment of the premium tax credit (APTC) and cost-sharing reductions (CSR), and certificates of exemption from the individual responsibility requirements. This program requires determinations of whether an individual is a citizen or national of and is lawfully present in the United States, whether an individual meets the income threshold for APTC and CSR, whether an individual's employer-sponsored health insurance is unaffordable, and whether to grant a certification that an individual is entitled to an exemption from the individual responsibility and/or penalty under Section 5000A of the Internal Revenue Code of 1986 (Code).
9. Section 1411(c) of the ACA requires that a Marketplace submit certain applicant information to the Secretary of Health and Human Services (HHS) for verification with other specified federal agencies. Section 1411(d) requires the Secretary of HHS to provide for verification of other applicant information in a manner as the Secretary determines appropriate. Section 1411(e) requires that the verifying entity report the response to the information submitted under 1411(c) and (d) to the Secretary of HHS in the manner the HHS Secretary determines is appropriate and requires that the HHS Secretary notify the Marketplace of the results. The HHS Secretary has implemented these provisions for Marketplaces in 45 C.F.R. Part 155, subpart D.
10. Section 1411(c)(4)(A) of the ACA requires that the HHS Secretary, in consultation with the Secretary of the Department of the Treasury, the Commissioner of the Social Security Administration, and the Secretary of the Department of Homeland Security, provide that the verifications and determinations under Section 1411 are done through an online or other electronic system or another method approved by the Secretary of HHS.
11. Section 1411(f) of the ACA requires the Secretary to provide for periodic Redeterminations of eligibility and appeals of Eligibility Determinations. The HHS Secretary has implemented these requirements for Marketplaces in 45 C.F.R. Part 155.
12. Section 1413 of the ACA authorizes the Secretary of HHS to establish a system under which individuals may apply for enrollment in, and receive a determination of eligibility for participation in Insurance Affordability Programs or for enrollment in a Qualified Health Plan through an Exchange (without receipt of APTC or CSR). Specifically, section 1413(c) requires that the agencies administering these programs participate in an electronic data matching program for determining eligibility for participation, consistent with the standards set forth by the HHS Secretary, upon the basis of reliable, third party data. Section 1413(d) of the ACA grants the HHS Secretary the authority to establish model agreements and to enter into agreements for the data sharing under this section, subject to Section 1411 of the ACA and Section 6103(l)(21) of the Code. 42 C.F.R. §§ 435.949 and 457.380(g), implementing Section 1413, provides that state agencies administering Medicaid and CHIP must use an electronic service established by HHS Secretary to verify information to the extent that information is available through the electronic service. The Federal Data

Services Hub is such a service.

13. Section 1331 of the Affordable Care Act authorizes States to establish BHPs, and BHP regulations require that states administering BHPs verify whether an individual meets the eligibility requirements in Section 1331(e) for enrollment in a BHP. BHPs also require periodic Redeterminations of eligibility and the opportunity to appeal denials of eligibility under 42 CFR 600.335.
14. Medicaid and CHIP programs require periodic Renewals and Redeterminations of eligibility for those programs and the opportunity to appeal denials of eligibility under Sections 1902(a)(8) and 1902(a)(3) of the Social Security Act and 42 C.F.R. §§ 435.916, 457.343 and Part 431, Subpart E and Part 457 Subpart K. Pursuant to 42 C.F.R. § 435.945 and 42 C.F.R. § 457.348, a Medicaid or CHIP agency must disclose certain income and eligibility information, subject to regulations at 42 C.F.R. part 431, subpart F, needed for verifying eligibility for an Insurance Affordability Program.
15. 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 Insurance Affordability Programs and prohibits disclosure of Federal Tax Information to a Marketplace 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. "ACA" 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 ACA).
2. "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 Marketplace (SBM) established under Section 1311 of the ACA.
3. "applicable State health subsidy program" means the program under this title for the enrollment in qualified health plans offered through an Exchange, including the premium tax credits under section 36B of the Internal Revenue Code of 1986 and cost-sharing reductions under section 1402; a State Medicaid program under title XIX of the Social Security Act; CHIP under title XXI of such Act; and a State program under section 1331 establishing qualified BHPs.
4. "Applicant" means an individual who is seeking eligibility for him or herself through an application submitted to the 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.

5. "Application Filer" means the person filing an application for an Applicant. An Application Filer may be an Applicant; an adult who is in the Applicant's household, as defined in 42 CFR 435.603(f), or family, as defined in Section 36B(d)(1) of the Code; an individual who is liable for the shared responsibility payment in accordance with 26 CFR 1.5000A-1(c); an Authorized Representative of an Applicant; or if the Applicant is a minor or incapacitated, someone acting responsibly for the Applicant.
6. "APTC" means advance payments of the premium tax credit specified in Section 36B of the Code (as added by Section 1401 of the Affordable Care Act) which are provided on an advance basis on behalf of an eligible individuals enrolled in a Qualified Health Plan through a Marketplace in accordance with Sections 1402 and 1412 of the Affordable Care Act.
7. "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 C.F.R. §155.227 or for Medicaid at 42 C.F.R § 435.923.
8. "BHP" means an optional basic health program established under Section 1331 of the ACA.
9. "Breach" is defined by Office of Management and Budget (OMB) Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information, May 22, 2007, as the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, loss of control, or any similar term or phrase that refers to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.
10. "CHIP" means the Children's Health Insurance Program established under Title XXI of the Social Security Act.
11. "CMS" means the Centers for Medicare & Medicaid Services.
12. "CSR" means cost-sharing reductions for an eligible individual enrolled in a silver level plan through the Marketplace or for an individual who is an Indian enrolled in a QHP through the Marketplace.
13. "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 minimum essential coverage 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.
14. "Enrollee" means an individual or employee enrolled in a Qualified Health Plan through a Marketplace or in an Insurance Affordability Program.

15. “Exchange” and “Marketplace” mean an American Health Exchange established under Sections 1311(b), 1311(d), or 1321(c)(1) of the ACA, including both State-based Marketplaces (SBMs) and FFMs.
16. “FFM” means Federally Facilitated Marketplace, which is an Exchange established by HHS and operated by CMS under Section 1321(c)(1) of the ACA.
17. “Hub” or “Federal Data Services Hub” is the CMS federally-managed service to transmit data between Federal and State Administering Entities and to interface with Federal agency partners and data sources.
18. “Incident” means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices. This includes attempts (including both failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction. While certain adverse events, (e.g., floods, fires, electrical outages, excessive heat, etc.) can cause system crashes, they are not considered Incidents. An Incident becomes a Breach when there is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access to personally identifiable information or personal health information, whether physical or electronic.
19. “Insurance Affordability Programs” means (1) the program under title I of the ACA that makes available coverage in a Qualified Health Plan through a Marketplace with APTCs or CSRs; (2) a Medicaid program under title XIX of the Social Security Act; (3) a Children’s Health Insurance Program (CHIP) under title XXI of the Social Security Act; and (4) a program under Section 1331 of the ACA establishing qualified basic health plans.
20. “Medicaid” means the health insurance program established under Title XIX of the Social Security Act and is one of the Insurance Affordability Programs.
21. “Periodic data matching” means the periodic examination of data sources by an Administering Entity for current enrollees.
22. “PII” or “personally identifiable information” is defined by OMB Memorandum M-07-16 (May 22, 2007) and refers to 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.

23. "Qualified Health Plan (QHP)" means an insurance plan under the Affordable Care Act, that is certified by a Marketplace 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.
24. "Quarter of Coverage" (QC) is the basic unit of social security coverage used in determining a worker's insured status. SSA will credit an individual with QCs based on his/her earnings or self-employed net profit covered under social security. Certain States require that an Applicant who is a Lawful Permanent Resident have 40 QCs or more in order to be eligible for Medicaid in that State. Those QCs 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.
25. "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.
26. "Redetermination" means the process by which a Marketplace or a BHP makes an Eligibility Determination for an Enrollee in one of the following circumstances: (1) on an annual basis prior to a Marketplace open enrollment period; (2) on a periodic cycle (e.g., 12 months) tied to the date of the application; and/or (3) when an individual communicates an update to a Marketplace that indicates a change to the individual's circumstances affecting their eligibility.
27. "Relevant Individual" means any individual listed by name and Social Security Number (SSN) on the application whose personally identifiable information or financial information may bear upon an Eligibility Determination of an Applicant. CMS will not request citizenship or immigration status data for a Relevant Individual for whom an Eligibility Determination is not sought.
28. "Renewal" means the annual process for an Enrollee to be considered for continued coverage under a state Medicaid program or a state Children's Health Insurance Program.
29. "Return Information" or "Federal Tax Information (FTI)" means information as defined under Section 6103(b)(2)(A) of the Code and in IRS Publication 1075, as any information collected or generated by the IRS with regard to any person's liability or possible liability under the Code. It includes, but is not limited to, information, including the return, which IRS obtained from any source or developed through any means that relates to the potential liability of any person under the Code for any tax, penalty, interest, fine, forfeiture, other imposition or offense; information extracted from a return, including names of dependents or the location of business; taxpayer's name, address and identification number; information collected by the IRS about any person's tax affairs, even if identifiers such as name, address and identification number are deleted; status of whether a return was filed, under examination, or subject to other investigation or processing, including collection activities; and information contained on transcripts of accounts.
30. "State-based Exchange," "State-based Marketplace" or "SBM" means an Exchange established and operated by a State, and approved by HHS under 45 C.F.R. § 155.105.

31. "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 are not limited to CMS, the Internal Revenue Service (IRS), Social Security Administration (SSA), Department of Homeland Security (DHS), Department of Veterans Affairs (VA), Department of Defense (DOD), Peace Corps, Office Personnel Management (OPM), and commercial databases of income and employment, to support an Eligibility Determination.
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 VI of this Agreement.

### **B. Administering Entity Responsibilities:**

1. AE will only request data or data verifications from CMS that are necessary to make Eligibility Determinations as described under Section VI.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 VI of this Agreement.
3. AE will provide the data elements identified in Section VI, part 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, AEs may not use or disclose Federal Tax Information to any entity or

individual unless such disclosure is permitted under the Code and approved by the IRS.

5. Where AE is a Medicaid or CHIP agency in a state where the FFM 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 Marketplace, Medicaid, and CHIP, and the Disclosure of Certain Data Obtained through the Data Services Hub" issued to AE's by CMS, which is specifically incorporated by reference in this Computer Matching Agreement and attached hereto as Attachment C.

### **III. JUSTIFICATION AND ANTICIPATED RESULTS**

#### **A. Justification**

The Affordable Care Act requires the use of a single, streamlined application which may be used to apply for an Eligibility Determination for enrollment in an Insurance Affordability Program or a Qualified Health Plan (without APTC or CSR) through a Marketplace.

An Applicant may be able to file the application for enrollment in an Insurance Affordability Program or enrollment in a Qualified Health Plan (without APTC or CSR) through a Marketplace online, by telephone, in person, or by mail with any of the entities administering these programs. The ability of an Applicant to access the appropriate coverage across multiple programs through a single streamlined application and coordinated eligibility process means that no matter how an application is submitted or which entity receives the application data, an Applicant will experience a consistent process and receive a consistent Eligibility Determination, without the need to submit information to multiple programs. In addition, on a periodic basis, Enrollees' eligibility for the applicable Insurance Affordability Program or a Qualified Health Plan (without APTC or CSR) will be re-determined or renewed.

Some individuals may be exempt from the requirement to maintain minimum essential coverage or the individual shared responsibility payment, including someone who's religious beliefs conflict with acceptance of the benefits of private or public insurance and those who do not have an affordable health insurance coverage option available. Depending on the exemption, an Applicant or Application Filer will either file a separate application to determine eligibility for an exemption and submit it to the Marketplace, or other location as directed on the application, or claim the exemption when filing their federal income tax return with the Internal Revenue Service by completing Form 8965.

It has been determined by the Parties that a computer matching program is the most efficient and expeditious means of obtaining and processing the information needed by AEs to support Eligibility Determinations, or to carry out general program administration as required by statute or regulations as specifically authorized in Section VI of this Agreement. This matching program will enable AEs to verify information in order to complete an Eligibility

Determination while complying with applicable laws about use of an electronic service and the role of HHS.

#### B. Anticipated Results

CMS anticipates that this matching program will produce expedited Eligibility Determinations and will reduce cost and minimize administrative burdens. The benefit of this data match with respect to Insurance Affordability Programs is the increased assurance that CMS and AEs achieve efficiencies and administrative cost savings to Insurance Affordability Programs and Marketplaces. This collaborative model, which offers service-based access to data for verification purposes and for Eligibility Determinations, or to carry out general program administration as required by statute or regulations specifically authorized in Section VI of this Agreement, will lessen financial and administrative burdens by eliminating the need for each State and each AE to execute several agreements with multiple federal agencies and other data sources.

#### C. Cost Benefit Analysis

Section 552a(u)(4) of the Privacy Act provides that a cost-benefit analysis must be completed prior to the approval of this Agreement. In addition to the computer matching program subject to this Agreement, CMS has computer matching agreements with federal agencies and Administering Entities under which CMS receives data matches through the Hub from multiple source agencies, and CMS and Administering Entities access data matches for the purpose of making Eligibility Determinations related to enrollment in a Qualified Health Plan or Insurance Affordability Program. CMS has conducted one cost-benefit analysis covering these computer matching agreements. This cost-benefit analysis is attached as Attachment B.

### **IV. DESCRIPTION OF THE DATA TO BE EXCHANGED**

The Privacy Act requires that each Computer Matching Agreement specify a description of the records which will be matched and exchanged, including a sample of data elements that will be used and the approximate number of records that will be matched. Specific lists of data elements for each Hub service are described in detail in relevant Data Services Hub Business Service Definition documents found on the Collaborative Application Lifecycle Tool (CALT) website maintained by CMS, which AEs have access to.

#### A. Systems of Records

The CMS Privacy Act System of Records Notice (SORN) that supports this matching program is the CMS Health Insurance Exchanges (HIX) Program, CMS System No. 09-70-0560, as amended, published at 78 Fed. Reg. 8538 (February 6, 2013), 78 Fed. Reg. 32256 (May 29, 2013) and Fed. Reg. 63211 (October 23, 2013).

#### B. Number of Records

The Congressional Budget Office (CBO) estimated that up to 33 million people may enroll for coverage in Qualified Health Plans and other Insurance Affordability Programs in calendar year 2016.

### C. Records Description

1. From AEs to CMS. AEs 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 Qualified Health Plan through a Marketplace, 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.
  
2. From CMS to AEs. 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 minimum essential coverage
  - e. Income, based on Federal Tax Information, Title II benefits, and current income sources
  - f. Quarters of Coverage
  - g. Death Indicator
  
3. Exact data elements sent to CMS and returned by CMS will vary by query and AE. These data outputs, and the manner of transfer developed by the Secretary, are captured in Data Services Hub Business Service Definitions, organized by information technology (IT) business service. The following IT business services have been identified for the purposes outlined in this Agreement:
  - a. SSA Composite (includes SSN validation, indication of death, incarceration, Title II benefits, and quarters of coverage).

This service is available to all AEs.

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

This service is available to all AEs.

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

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

- d. Verify Current Income from other sources.

This service is available to all AEs.

- e. Verify Employer-Sponsored Insurance (ESI) Minimum Essential Coverage (MEC).

This service is available to all SBMs and BHPs.

- f. Verify Non-ESI MEC.

(1) Medicaid/CHIP can use this service to verify Medicare MEC.

(2) SBMs 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).

This service will be available to all AEs, but is specifically designed for use by State-based Marketplaces for periodic checks of current enrollees.

- h. Redetermination & Renewal Verification Bulk Service (includes IRS income, SSA Title II benefit income, current income, and Medicare MEC).

This service is available to all AEs. IRS income is available only for AEs authorized to receive Federal Tax Information from the IRS.

- 4. To the extent the AE is required under 45 CFR Subpart D to use the services described in VI.C.3, or otherwise opts to use the services and is approved to do so by CMS, the AE must adhere to the requirements and limitations that are described in VI.C.5 below for each service.

- 5. The following describe the Hub services that are available to AEs, circumstances under which those services may or may not be called, and/or the purposes for which data from that service may be used:

- a. SSA Composite:

(1) This service may only be called for initial eligibility determinations and mid-year redeterminations based on applicable reported changes, or any appeal process

related to a determination.

- (2) The service may not be called for periodic data matching to conduct verifications for general program integrity purposes, but only periodic data matches described under 45 C.F.R. § 155.330(d).
- (3) The citizenship verification component of this service may only be called for Applicants who have attested to being citizens or nationals. Once citizenship of an Applicant has been verified by the AE, it should not be re-verified unless there is a reported change in citizenship status.
- (4) The incarceration component of this service may only be called to the extent it is necessary to determine eligibility for enrollment in a QHP, an Insurance Affordability Program. AEs that are Medicaid/CHIP agencies may also call this service to comply with program requirements.
- (5) The Quarters of Coverage component of this service may only be called to the extent it is necessary to make an initial determination of an individual's eligibility or a determination of an individual's eligibility based on a change to an individual's circumstances that is reported to the AE.
- (6) The AE may attempt to validate the SSN no more than 3 times in a 24 hour period.

**b. Verify Lawful Presence:**

- (1) This service may only be called for initial eligibility determinations and mid-year redeterminations based on applicable reported changes, or any appeal process related to a determination.
- (2) This service may not be called automatically re-verify immigration status to support mid-year or annual redeterminations using this service unless the AE has reason to believe the status is subject to change.
- (3) If an AE is unable to comply with prompts for additional verification sent from DHS through the Hub, the AE must implement an approved alternative verification method which may require an AE to review documents that demonstrate the applicants' immigration status. If possible, alternative verification methods should use the AE's independent DHS/USCIS Systematic Alien Verification for Entitlements (SAVE) Program 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.
- (4) AEs agree not to deny eligibility for a program covered under this Agreement based upon the failure to verify applicant information with DHS records unless an

AE completes all SAVE prompts returned via the Hub, including submitting the verification request for additional verification or resubmitting the case when prompted by SAVE, or completes an alternate verification procedure as described in VI(C)(5)(b)(3).

**c. Income and Family Size Verification:**

- (1) This service may only be called for initial eligibility determinations and mid-year redeterminations based on applicable reported changes and determinations with consent of the Applicant, for up to five years.
- (2) The AE may only call for mid-year redeterminations based on applicable reported changes, including an applicant's report of tax filing status.
- (3) The AE may only send requests containing validated SSNs.
- (4) The AE may not call this service to obtain income information to support an eligibility appeal. FTI in an appellant's eligibility record may not be disclosed to his/her designated representative or any other member of the individual's household who may be involved in the proceeding absent appropriate authorization from the Relevant Individual.

**d. Verify Current Income from other sources:**

This service may only be called for initial eligibility determinations and mid-year redeterminations based on applicable reported changes, or any appeal process related to a determination.

**e. Non-ESI MEC:**

This service may only be called for initial eligibility determinations and mid-year redeterminations based on applicable reported changes, as defined in III.X, or any appeal process related to an Eligibility Determination.

**f. Verify Employer-Sponsored Insurance (ESI) Minimum Essential Coverage (MEC):**

This service may only be called for initial eligibility determinations and mid-year redeterminations based on applicable reported changes, or any appeal process related to a determination.

**g. Periodic Eligibility Verifications (Bulk Service):**

This service may be used by AEs that are SBMs or BHPs to periodically verify whether an Enrollee has become Medicare eligible or deceased since the last verification occurred. AEs must use this service, not the synchronous services listed above, to support periodic data matching that does not meet the description under 45 C.F.R. § 155.330(d), unless otherwise authorized by CMS.

**h. Redetermination & Renewal Verification (Bulk Service):**

Data from this bulk service must be used for annual redeterminations and Renewals. Accordingly, AEs must use this service to support annual redeterminations and Renewals, not the synchronous services listed above, unless otherwise authorized by CMS.

**V. PROCEDURES FOR INDIVIDUAL NOTICE**

The Privacy Act requires that each matching agreement specify procedures for providing individualized notice at the time of application, as required by 5 U.S.C. § 552a(o).

- A. CMS will publish notice of the matching program in the Federal Register (FR) as required by the Privacy Act (5 U.S.C. § 552a(e)(12)).
- B. At the time of application, AEs 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 SBM will make the Eligibility Determination for the exemption itself or whether the SBM will utilize the federally managed service to make the Eligibility Determination for an exemption, the SBM 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.
- C. At the time of Redetermination, SBMs 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 C.F.R. §435.916 and 42 C.F.R. §457.343.

**VI. VERIFICATION AND OPPORTUNITY TO CONTEST**

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

- A. Correcting information with a relevant data source is not necessary to resolve inconsistencies or complete an Eligibility Determination. Resolving an inconsistency with an AE will not correct information contained in the records of the relevant data source.

Any information provided via the Hub by other data sources, or 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 a Marketplace 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 Internal Revenue Service.

- B. 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 they provided did not match information received through electronic verifications as follows:
1. If the AE is a Marketplace, 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 inconsistencies between attestations and the results of electronic 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 Marketplace verification procedures at 45 CFR §§ 155.315 and 155.320, or Medicaid verification procedures at 45 CFR § 435.945-956; and will resolve inconsistencies as set forth in Paragraphs VIII.B.1. and 2 above.

## **VII. ACCURACY ASSESSMENTS**

Accuracy rates of information provided through the Hub are affirmed in computer matching agreements between CMS and the Federal Agencies providing the data.

## **VIII. RETENTION OF RECORDS**

Administering Entities will retain all records received from the exchange of the matched data received under this Agreement (and all personally identifiable data derived from the matched data) for a period of ten (10) years.

## **IX. SAFEGUARDS AND PRIVACY AND SECURITY INCIDENT REPORTING**

### **A. Safeguards**

1. An AE shall comply with all applicable regulations regarding the privacy and security of

PII (see e.g., Section 1411(g) of the ACA, 45 C.F.R. § 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 C.F.R. 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)).

2. An AE 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 AEs must comply. Further, AEs 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.
3. An AE shall ensure that its employees, contractors, and agents:
  - a. 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.
  - b. 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.
  - c. Ensure that laptops and other electronic devices/media containing matching data that

constitutes PII are encrypted and/or password protected.

- d. Send emails containing matching data that constitutes PII only if encrypted and being sent to and received by email 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 emailing Return Information.
- e. Restricted access to the matching data 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.
- f. For receipt of Federal Tax Information, AEs 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 AEs to which CMS provides return information to:
  - (1) 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.
  - (2) 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.
  - (3) 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.

- (4) 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.
- (5) Prior to initial access to FTI and annually thereafter, AE will ensure that 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 sections 7213, 7213A, and 7431 of the Code for any willful disclosure or inspection of Return Information that is not authorized by the Code, in accordance with Publication 1075, section 6.0.
- (6) Prior to initial receipt of Return Information, have an IRS approved Safeguard Security Report (SSR). Each AE must annually thereafter submit an SSR. Each Administering Entity'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 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. SSRs 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.
- (7) 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.
- (8) 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.

- (9) Each Administering Entity must ensure information systems processing return information are compliant with Section 3544(a)(1)(A)(ii) of the Federal Information Security Management Act of 2002 (FISMA). Each Administering Entity 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.
- (10) Each Administering Entity agrees to 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.
- (11) CMS must ensure that contracts with contractors and subcontractors performing work involving return information under this agreement contain specific language requiring compliance with IRC section 6103(p)(4) and Publication 1075 safeguard requirements and enforces CMS' right to, and permits IRS access to, contractor and subcontractor facilities to conduct periodic internal inspections where return information is maintained to ensure IRS safeguarding requirements are met.
- (12) 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.
- (13) IRS will 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.
- (14) 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.

## B. Incident Handling and Reporting

1. AEs are responsible for creating their 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. AEs shall handle and report Incidents in accordance with their 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 personally identifiable information (PII).
  - b. Report all suspected or confirmed Incidents involving matching data that constitute PII. This requirement applies to all system environments (e.g., production, pre-production, test, development).
  - c. 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.
  - e. 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.
  - f. 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. AEs 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. SBMs and BHPs report a Security Incident or Breach of PII to

[HIX.incidents@cms.hhs.gov](mailto:HIX.incidents@cms.hhs.gov) within one hour of discovery of the Incident by completing incident form (CALT doc53607). That email 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 SBM 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 SBM must immediately contact the CMS IT Service Desk at (410) 786-2580 or via email at [CMS\\_IT\\_Service\\_Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov).

- b. SBMs and BHPs report any Incident involving Federal Tax Information (FTI) to the Internal Revenue Service (IRS) Office of Safeguards by email to [safeguardreports@irs.gov](mailto:safeguardreports@irs.gov). Additionally, SBMs must telephone the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-589-3718. SBMs should not wait until after their own internal investigation has been conducted to report an incident to CMS, TIGTA, and the IRS.
  - c. Medicaid and CHIP agencies operating in a state in which the FFM 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 Federal Tax Information (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 Section 10.1, IRS Publication 1075, <http://www.irs.gov/pub/irs-pdf/p1075.pdf>
  - d. A Medicaid and/or a CHIP agency, when operating as an AE performing Exchange functions under a State-based Marketplace, report to [HIX.Incidents@cms.hhs.gov](mailto: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/Medicaid and/or CHIP agency shall contact 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 Federal Tax Information. 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 C.F.R. 431.300-431.306 and 435.945.
3. AEs shall refer to the Interconnection Security Agreement (ISA) for instructions on handling disconnects from the Federal Services Data Hub (FDSH). The Change

Management section provides instructions for handling an emergency or planned disconnect, initiated by the AE or CMS, as well as restoration procedures.

**C. Administering Entity Opt Out for Receiving FTI**

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

**X. 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 system of records notices (SORNs) or Federal law.
- C. The matching data exchanged under this Agreement remain the property of the Party that provided the data and will be retained and destroyed as described in Section X of this matching Agreement.
- D. CMS and AEs will restrict access to data solely to officers, employees, and contractors of CMS and AEs.
- E. The AE will restrict access to the matching data to Applicants, Enrollees, Application Filers, and Authorized Representatives of such persons. AEs shall execute with each individual or entity such as agents or brokers that (1) gain access from the AE to PII submitted to a Marketplace 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 C.F.R. §431, subpart F, including §§431.301, 431.302, 431.303, 431.305, and 435.945, and 42 CFR 457.1110.

- F. Any individual who receives information from a Marketplace 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 C.F.R. § 155.260 and Section 1411(g) of the ACA are potentially subject to the civil penalty provisions of Section 1411(h)(2) of the ACA and 45 C.F.R. §155.285, which carries a fine of up to \$25,000.

#### **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 and AE records, as necessary, in order to verify compliance with this Agreement.

#### **XII. REPORT TO CONGRESS AND OMB**

When the State and the CMS Data Integrity Board (DIB) have approved this Agreement, CMS will submit a report of the matching program to Congress and OMB for review, and will provide a copy of such notification to the Administering Entity.

#### **XIII. REIMBURSEMENT**

Neither Party will receive reimbursement as part of this Agreement.

#### **XIV. INTEGRATION CLAUSE**

This Agreement, including incorporations by reference, 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 CMS and AEs for the purposes described in this Agreement. Neither Party has made representations, warranties, or promises outside of this Agreement. This Agreement takes precedence over any other documents that may be in conflict with it.

#### **XV. SEVERABILITY**

If any term or other provision of this Agreement is determined to be invalid, illegal or incapable of being enforced by any rule or law, or public policy, all other terms, conditions, or provisions of this Agreement shall nevertheless remain in full force and effect, provided that the data exchange program contemplated hereby is not affected in any manner materially adverse to any Party. Upon such determination that any term or other provision is invalid, illegal or incapable

of being enforced, the Parties hereto shall negotiate in good faith to modify this Agreement so as to effect the original intent of the Parties as closely as possible in an acceptable manner to the end that the transactions contemplated hereby are satisfied to the fullest extent possible.

**XVI. PERSONS TO CONTACT**

**A. The CCIIO/EPOG contact for Programmatic issues:**

Elizabeth Kane  
Acting Director, Verifications Policy & Operations Division  
Eligibility and Enrollment Policy and Operations Group  
Center for Consumer Information and Insurance Oversight  
Centers for Medicare & Medicaid Services  
7501 Wisconsin Avenue  
Bethesda, MD 20814  
Telephone: (301) 492-4418  
Email: [elizabeth.kane@cms.hhs.gov](mailto:elizabeth.kane@cms.hhs.gov)

**The CCIIO/SEG contact for Programmatic issues:**

Jenny Chen  
Director, Division of State Technical Assistance  
State Exchange Group  
Center for Consumer Information and Insurance Oversight  
Centers for Medicare & Medicaid Services  
7501 Wisconsin Avenue  
Bethesda, MD 20814  
Telephone: 301-492-5156  
Email: [Jenny.Chen@cms.hhs.gov](mailto:Jenny.Chen@cms.hhs.gov)

**The Medicaid/CHIP contact for Programmatic issues:**

Jessica Kahn  
Director, Data Systems Group  
Center for Medicaid and CHIP Services  
Centers for Medicaid & Medicare Services  
Baltimore, MD 21244-1850  
Phone: (410) 786-9361  
E-Mail: [Jessica.Kahn@cms.hhs.gov](mailto:Jessica.Kahn@cms.hhs.gov)

**The CMS contact for Privacy Policy and agreement issues:**

Walter Stone  
CMS Privacy Officer  
Division of Security, Privacy Policy and Governance  
Information Security and Privacy Group  
Office of Enterprise Information  
Centers for Medicare & Medicaid Services

7500 Security Boulevard  
Mail Stop: S2-24-25  
Baltimore, MD 21244-1850  
Telephone: (410)786-5357  
E-mail: [walter.stone@cms.hhs.gov](mailto:walter.stone@cms.hhs.gov).

The CMS contact for Systems Operations:

Darrin V. Lyles  
Information Security Officer, RPDG  
CMS\OIS\RPDG  
Consumer Information and Insurance Systems Group  
7500 Security Boulevard  
Baltimore, MD 21244  
Phone: 410-786-4744  
Phone: 443-979-3169 (Mobile)  
E-mail: [Darrin.Lyles@cms.hhs.gov](mailto:Darrin.Lyles@cms.hhs.gov)

The CMS contact for Privacy Incident Reporting:

LaTasha Grier  
Division of Cyber Threat & Security Operations  
Division of Information Security, Privacy Policy & Governance  
Information Security & Privacy Group  
Office of Enterprise Information  
Centers for Medicare & Medicaid Services  
7500 Security Boulevard  
Mail Stop: N1-24-08  
Baltimore, MD 21244-1849  
Telephone: (410) 786-3328  
E-mail: [LaTasha.Grier@cms.hhs.gov](mailto:LaTasha.Grier@cms.hhs.gov).

The CMS contact for Security Issues:

Devany Nicholls  
Baltimore Data Center ISSO  
Division of Operations Management  
Enterprise Infrastructure & Operations Group  
Office of Technology Solutions  
7500 Security Boulevard  
Baltimore, MD 21244-1859  
Phone: (410) 786-8189  
Fax: (410) 786-9700  
E-mail: [Devany.Nicholls@cms.hhs.gov](mailto:Devany.Nicholls@cms.hhs.gov)

B. The CMS contact person for Privacy Incident Reporting issues:

States should refer questions to their designated CMS State Officer.

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

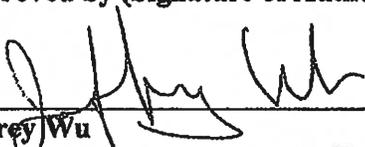
## **XVII. EFFECTIVE DATE, TERM, MODIFICATION, AND TERMINATION**

- A. **Effective Date:** The Effective Date of this Agreement is April 2, 2016, provided that the following review periods have lapsed: thirty (30) days from the date CMS publishes a Notice of Computer Matching in the Federal Register; thirty (30) days from the date the matching program report is transmitted to the Congressional committees of jurisdiction consistent with the provisions of 5 U.S.C. §§ 552a (r), (o)(2)(A), and (o)(2)(B); and forty (40) days from the date the matching program report is sent to OMB, consistent with the provisions of 5 U.S.C. § 552a (r) and OMB Circular A-130, Revised (Transmittal Memorandum No. 4), November 28, 2000, Appendix I, entitled "Federal Agency Responsibilities for Maintaining Records about Individuals" (A-130 Appendix I).
- B. **Term:** The initial term of this Agreement will be eighteen (18) months.
- C. **Renewal:** 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 can certify the following to the HHS DIB or appropriate governance body:
1. The matching program will be conducted without change; and
  2. CMS and AE have conducted the matching program in compliance with the original Agreement.
- D. **Modification:** The Parties may modify this Agreement at any time by a written modification, mutually agreed to by both Parties and approved by the HHS DIB.
- E. **Termination:** This Agreement may be terminated at any time upon the mutual written consent of the Parties. If either Party does not want to extend this Agreement, it should notify the other at least ninety (90) days prior to the expiration of this Agreement.

**XVIII. APPROVALS**

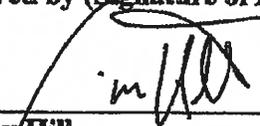
**A. Centers for Medicare & Medicaid Services Program Official**

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.

<b>Approved by (Signature of Authorized CMS Program Official)</b>	
	
<b>Jeffrey Wu</b> <b>Associate Deputy Director for Policy</b> <b>Center for Consumer Information and Insurance Oversight</b> <b>Centers for Medicare &amp; Medicaid Services</b>	<b>Date:</b> 02/19/76.

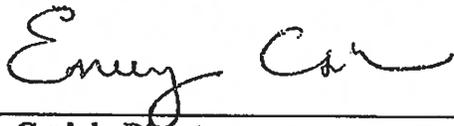
B. Centers for Medicare & Medicaid Services Program Official

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.

<b>Approved by (Signature of Authorized CMS Program Official)</b> 	
<b>Timothy Hill</b> <b>Deputy Director</b> <b>Center for Medicaid and CHIP Services</b> <b>Centers for Medicare &amp; Medicaid Services</b>	<b>Date:</b> 2/19/16

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.

<b>Approved By (Signature of Authorized CMS Approving Official)</b>	
	
<b>Emery J. Csulak, Director Information Security and Privacy Group &amp; Senior Official for Privacy Offices of Enterprise Information Centers for Medicare &amp; Medicaid Services</b>	<b>Date:</b>  2-3-16

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.

<b>Approved By (Signature of Authorized HHS DIB Official)</b>	
	
<b>Colleen Barros</b> <b>Chairperson, HHS Data Integrity Board</b> <b>Acting Assistant Secretary for Administration</b> <b>U.S. Department of Health and Human Services</b>	<b>Date:</b>  3/1/16

E. Participating Administering Entity Program Official

1. Administering Entity Model

The Administering Entity will request via the Hub information necessary to make 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 Administering Entity, and then transmit the results of the data match back to the Administering Entity.

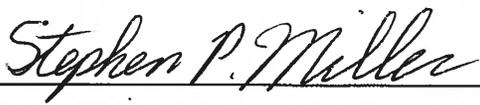
The Administering Entity under this Agreement is: (Check all that apply.)

- Medicaid Agency
- Children's Health Insurance Program
- Basic Health Program
- State-based Marketplace

The Administering Entity will determine eligibility for the following: (Check all that apply.)

- 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 Administering Entity 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 his/her respective organization to the terms of this Agreement.

<b>Approved by (Signature of Authorized Administering Entity Official)</b>	
	
<b>(Insert name and Title of person signing for the Administering Entity)</b>	<b>Date:</b> 3/23/16

Attachment A: Proposed Federal Register Notice

Attachment B: Proposed Master Cost Benefit Analysis (CBA)

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

ATTACHMENT A

Billing Code: 4120-03

**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**

**Computer Matching Agreement No. 2016-11  
The Department of Health and Human Services No. 1601**

**Effective Date – April 2, 2016  
Expiration Date – October 2, 2017**

**AGENCY:** Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS)

**ACTION:** Notice of Computer Matching Program (CMP)

**SUMMARY:** In accordance with the requirements of the Privacy Act of 1974, as amended, this notice announces the establishment of a CMP that CMS plans to conduct with the State-Based Administering Entities.

**EFFECTIVE DATES:** Comments are invited on all portions of this notice. Submit public comments on or before April 1, 2016. The matching program will become effective no sooner than 40 days after the report of the matching program is sent to the Office of Management and Budget (OMB) and a copy of the Agreement is sent to Congress, or 30 days after publication in the *Federal Register*, whichever is later.

**ADDRESS:** The public should send comments to: CMS Privacy Officer, Division of Security, Privacy Policy and Governance, Information Security and Privacy Group, Offices of Enterprise Information, CMS, Room N1-24-08, 7500 Security Boulevard, Baltimore, Maryland 21244-1850. Comments received will be available for review at this location, by appointment, during regular business hours, Monday through Friday from 9:00 a.m. - 3:00 p.m., Eastern Time zone.

**FOR FURTHER INFORMATION CONTACT:** Elizabeth Kane, Director, Verifications Policy and Operations Branch, Eligibility and Enrollment Policy and Operations, Center for Consumer Information and Insurance Oversight, Centers for Medicaid & Medicare Services, Phone: (301) 492-4418 or Email: [elizabeth.kane@cms.hhs.gov](mailto:elizabeth.kane@cms.hhs.gov).

**SUPPLEMENTARY INFORMATION:** The Computer Matching and Privacy Protection Act of 1988 (Public Law (Pub. L.) 100-503), amended the Privacy Act (5 U.S.C. § 552a) by describing the manner in which computer matching involving Federal agencies could be performed and adding certain protections for individuals applying for and receiving Federal benefits. Section 7201 of the Omnibus Budget Reconciliation Act of 1990 (Pub. L. 101-508) further amended the Privacy Act regarding protections for such individuals. The Privacy Act, as amended, regulates the use of computer matching by Federal agencies when records in a system of records are

matched with other Federal, state, or local government records. It requires Federal agencies involved in computer matching programs (CMP) to:

1. Negotiate written agreements with the other agencies participating in the matching programs;
2. Obtain the Data Integrity Board approval of the match agreements;
3. Furnish detailed reports about matching programs to Congress and OMB;
4. Notify applicants and beneficiaries that their records are subject to matching; and,
5. Verify match findings before reducing, suspending, terminating, or denying an individual's benefits or payments.

This matching program meets the requirements of the Privacy Act of 1974, as amended.

Date \_\_\_\_\_

\_\_\_\_\_  
Walter Stone

CMS Privacy Officer

Centers for Medicare & Medicaid Services

**CMS Computer Match No. 2016-11**

**HHS Computer Match No. 1601**

**Name:** "Computer Matching Agreement between the Department of Health and Human Services, Centers for Medicare & Medicaid Services and the State-Based Administering Entities for Determining Eligibility for Enrollment in Applicable State Health Subsidy Programs under the Patient Protection and Affordable Care Act."

**SECURITY CLASSIFICATION:**

Unclassified

**PARTICIPATING AGENCIES:**

Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS), and the State-Based Administering Entities.

**AUTHORITY FOR CONDUCTING MATCHING PROGRAM:**

Sections 1411 and 1413 of the Patient Protection and Affordable Care Act of 2010 (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152) (collectively, the ACA) require the Secretary of HHS to establish a program for applying for and determining eligibility for enrollment in applicable State health subsidy programs and authorizes the use of secure, electronic interfaces and an on-line system for the verification of eligibility.

The Computer Matching and Privacy Protection Act of 1988 (CMPPA) (Public Law 100-503),

amended the Privacy Act (5 U.S.C. § 552a) and requires the parties participating in a matching program execute a written agreement specifying the terms and conditions under which the matching will be conducted. CMS has determined that status verification checks to be conducted by the Federally-facilitated Exchange (FFE), and State-based Administering Entities using the data transmitted through the Federal Data Services Hub constitute a "computer matching program" as defined in the CMPPA.

**PURPOSE(S) OF THE MATCHING PROGRAM:**

The purpose of the Computer Matching Agreement is to establish the terms, conditions, safeguards, and procedures under which CMS will disclose certain information to State-based Administering Entities in accordance with the Patient Protection and Affordable Care Act of 2010 (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act (Public Law 111-152), which are referred to collectively as the Affordable Care Act (ACA), amendments to the Social Security Act made by the ACA, and the implementing regulations. The Administering Entities will use the data, accessed through the Hub, to make Eligibility Determinations for enrollment in an applicable State health subsidy program. This Computer Matching Agreement also establishes the terms, conditions, safeguards, and procedures under which State Medicaid/CHIP agencies shall provide data to CMS (as the Federally-facilitated Marketplace (FFM)), State-based Marketplaces (SBMs) and BHPs to verify whether an Applicant or Enrollee who has submitted an application to the FFM or an SBM has current eligibility or enrollment in a Medicaid/CHIP program.

**DESCRIPTION OF RECORDS TO BE USED IN THE MATCHING PROGRAM:**

This computer matching program will be conducted with data maintained by CMS in the Health

Insurance Exchanges (HIX) Program, CMS System No. 09-70-0560, as amended. The system is described in System of Records Notice published at 78 Federal Register 63211 (Oct. 23, 2013).

**INCLUSIVE DATES OF THE MATCH:**

This computer matching program will become effective no sooner than 40 days after the report of the matching program is sent to OMB and Congress, or 30 days after publication in the *Federal Register*, whichever is later. The matching program will continue for 18 months from the effective date and may be extended for an additional 12 months thereafter, if certain conditions are met.

## ATTACHMENT B

### Cost-Benefit Analysis: Eligibility Verifications with Federal Agencies

#### I. BACKGROUND

##### *Statutory Requirements*

This cost-benefit analysis covers computer matching programs used by CMS to provide “eligibility verification” hub services required to implement provisions of the Patient Protection and Affordable Care Act (ACA) related to verifying individuals’ eligibility for enrollment in qualified health plans (QHPs) with or without advance payments of the premium tax credit or cost-sharing reductions; in Medicaid; in CHIP; or in Basic Health Plans. Section 1411(a) of ACA requires the Secretary of the Department of Health and Human Services (HHS) to establish a program to determine eligibility for enrollment in coverage under a qualified health plan through an Exchange or certain state health subsidy programs<sup>1</sup>, and for certifications of exemption from the individual responsibility requirement or the penalty imposed by section 5000A of the Internal Revenue Code. Section 1411(c) requires the verification of certain identifying information against the records maintained the Social Security Administration, the Department of Homeland Security, and the U.S. Department of the Treasury. Section 1411(d) directs HHS to establish a system for the verification of other information necessary to make an eligibility determination. Section 1413 requires HHS to establish a streamlined enrollment system and secure electronic interface to verify data and determine eligibility for state health subsidy programs. Section 2201 requires that Medicaid and CHIP agencies utilize this streamlined enrollment system.

##### *Design of Computer Matching Program*

To implement these provisions regarding verifying consumer information related to eligibility determinations, CMS selected a computer matching program design that minimizes burdens for all parties and better ensures the integrity and security of the data. Specifically, CMS enters into separate CMAs with each of the following federal agencies: Social Security Administration (SSA), Department of Homeland Security (DHS), Internal Revenue Service (IRS), Veteran’s Health Administration (VHA), the Department of Defense (DoD), the Office of Personnel Management (OPM) and the Peace Corps (each a trusted data source or TDS). These CMAs address with specificity the data provided by each federal agency to CMS for use by CMS and state-based entities administering state health subsidy programs (Administering Entities) in performing eligibility determinations. CMS receives data covered under these CMAs through the CMS Data Services Hub (Hub), which provides a single data exchange for Federal and State-based agencies administering state health subsidy programs to interface with Federal agency partners. Administering Entities can request data matches through this Hub

---

<sup>1</sup> State health subsidy programs means the program for the enrollment in qualified health plans offered through an Exchange, including the premium tax credits and cost-sharing reductions; a state Medicaid program; a state children’s health insurance program (CHIP); and a state program under section 1331 establishing qualified basic health plans.

pursuant to a separate CMA entered into between each state and the District of Columbia and CMS. CMS uses the same CMA for each state, with the CMA specifying the allowed uses of data elements shared through the Hub, depending on which state health subsidy program the state administers (e.g., the CMA only authorizes a state to use certain data to perform verifications related to Basic Health Programs if the state administers a basic health program). This CMA also provides for Medicaid and CHIP programs to provide data to CMS for use in eligibility determinations.

This design achieves efficiencies by allowing Administering Entities to access data matches from federal Trusted Data Sources without each Administering Entity having to execute separate CMAs with each Trusted Data Source. Furthermore, the use of the Hub to transmit information to perform data matches under the program ensures adherence to Federal and industry standards for security, data transport, and data safeguards as well as CMS policy for Exchanges, and makes it unnecessary for each state to develop and support separate verification processes through which they can receive, store, and secure the data provided by the source federal agencies. Additionally, this design ensures that all parties are using the same data to perform eligibility determinations, which better ensures data integrity.

#### *Methodology of Cost-Benefit Analysis*

Although the cost-benefit analysis of this computer matching program design is based on limited data and includes estimates that have not been confirmed by studies, it addresses all four key elements identified in GAO/PEMD-87-2 (i.e., Personnel Costs; Computer Costs; Avoidance of Future Improper Payments; and Recovery of Improper Payments and Debts). The analysis includes estimates of CMS's labor and system costs as both the recipient agency in relation to the aforementioned trusted data sources and recipient and source agency in relation to state-based administering entities; costs incurred by TDSs; and costs to Administering Entities (Medicaid/CHIP agencies, Marketplaces and agencies administering the Basic Health Program) to support the hub services. It also includes qualitative benefits to the parties, including clients and the public at large. Where data are unavailable to produce informed estimates, the analysis also describes types of costs and benefits that are not quantifiable at this time. At this time, the only quantified benefits are cost savings achieved by using the existing matching program instead of a manual process for eligibility verifications.

The timeframe for the analysis is fiscal year 2015 – which programmatically aligns with eligibility and enrollment activities during Open Enrollment 2015 through just before 2016 Open Enrollment. CMS anticipates that operational experience beyond 2015 will provide additional data from which other quantifiable benefits could be estimated for future cost-benefit analyses of this computer matching program.

The methodology used compares the costs and benefits of performing eligibility verifications manually, without computer matching (i.e., without the single, streamlined computer system mandated by the ACA, which depends on use of computer matching), versus electronically, with computer matching. The hypothetical manual process is one in which no electronic data would be used for verification and consumers would be required to submit paper documentation to verify data as specified in the ACA. Because CMS has no choice but to use computer matching to comply with the ACA mandate to provide a single, streamlined computerized eligibility verification process, this cost-benefit analysis also describes savings

realized by the choice of design used to effect the computer matching programs. However, we do not have data to quantify these savings at this time.

The methodology for specific estimates is described in the following section.

## II. COSTS

### Key Element 1: Personnel Costs

#### *For Agencies –*

Note: CMS serves as both a recipient agency (with respect to TDS and certain Medicaid/CHIP programs) and a source agency (with respect to Administering Entities). Many of CMS's costs cannot be cleanly attributed to its role as either a source or a recipient agency. Therefore we have listed all of CMS's personnel costs together in a separate category. In addition, certain Medicaid and CHIP agencies play a dual role, as a source and recipient agency. We have grouped their costs in the recipient agency category.

- **Source Agency:** We estimate that personnel costs for source agencies total approximately \$21.7 million. CMS does not collect information from each source agency about their personnel costs, therefore this estimate is built off personnel cost assumptions based on hub service context, TDS partnership history and known ongoing work. We believe a decentralized computer matching program would require source agencies to designate additional personnel to accommodate the burden of supporting separate computer matching programs with each state.
- **Recipient Agencies:** We estimate that the personnel costs associated with the computer matching program to recipient agencies (including State-based Marketplaces, Medicaid/CHIP agencies and Basic Health Programs) is \$215 million. We do not require recipient agencies to submit personnel costs to CMS. This estimate is based on assumptions from CMS operational engagement with these agencies. In contrast, a manual process would require additional personnel to manually review and verify consumer information. We estimate that a manual process would require just over one billion dollars in personnel costs to recipient agencies. This estimate is based off the cost of the current cost of manually verifying consumer information today for Marketplaces and the Basic Health Program. The Medicaid/CHIP cost is mitigated by the assumption that without the current Hub Medicaid/CHIP would use the decentralized data connections they had pre-ACA with TDSs. Overall however, a decentralized computer matching program would likely require recipient agencies to spend more on personnel costs than the existing matching program, but less than a manual process. We have not quantified the associated costs.
- **CMS:** We quantified two categories of personnel costs for CMS: (1) personnel costs associated with verification services generally and providing support to the TDSs; and (2) personnel costs associated with providing state-based Administering Entities with technical assistance. Note, that these estimates focus on the operational, technical and policy support to the eligibility verification services; they do not include all personnel costs associated with the computer matching program. For example, we have not included an estimate of costs associated with preparing the computer matching agreements. We estimate that the computer matching program includes personnel costs for category (1) of approximately

\$1.5 million, and for category (2) of approximately \$400,000. This estimate is based on current staffing from policy, operational and technical support teams and their contractors directly supporting the eligibility verification services, the source agencies and the recipient agencies. We believe a manual system would increase the personnel costs in category (1), but decrease the personnel costs devoted to state technical assistance, for a net increase in personnel costs of approximately \$200,000. We believe a decentralized computer matching program would similarly decrease the personnel costs related to state technical assistance to CMS (while significantly increasing these costs for source and recipient agencies), but would not result in significant savings in category (1), as CMS would continue to require roughly the same personnel to support the verifications services for the Federally-facilitated Marketplace (FFM), and would continue to provide similar support to TDSs. Additionally, certain personnel costs incurred by source agencies are transferred to CMS. We estimate these computer costs at \$2.1 million. These costs were not included in the personnel costs estimated for source agencies above.

- *Justice Agencies:* Because, as described in section III, data from this computer matching program is not used to recover improper payments, we are aware of no personnel costs to justice agencies associated with this computer matching program.

*For Clients:* When a data match conducted through the eligibility hub services identifies a data inconsistency, clients (consumers) are given an opportunity to produce documentation showing they are eligible for the applicable program. We believe that the centralized, electronic/real-time computer matching program produces more accurate verifications than either a manual system or a decentralized computer matching program, minimizing the amount of time clients must spend responding to inaccurate verifications. We have quantified that cost at \$408 million, using the estimated time to gather and mail documents and the standard hourly wage to quantify an average client's time. In addition to saving clients time, we believe the more efficient centralized computer matching program design will reduce the frustration experienced by clients in trying to verify their data.

*For Third Parties:* Although no data was developed regarding costs to third parties, we would expect that overall the increased accuracy of data matches achieved through this computer matching agreement would result in lower personnel costs to third parties. For example Navigators who assist consumers with an applicant, would have lower costs than they would with either a manual process or a decentralized computer matching program.

*For the General Public:* We are not aware of personnel costs to the general public associated with the matching program.

#### Key Element 2: Agencies' Computer Costs

Note: CMS serves as both a recipient agency (with respect to each TDS and certain Medicaid/CHIP programs) and a source agency (with respect to Administering Entities). Many of CMS's costs cannot be cleanly attributed to its role as either a source or a recipient agency. Therefore we have listed all of CMS's computer costs separately. In addition, certain Medicaid and CHIP agencies play a dual role, as a source and recipient agency. We have grouped their costs in the recipient agency category.

- *Source Agencies (with exception of CMS and Medicaid/CHIP agencies):* We estimate the computer costs associated with the computer matching program to be \$7.0 million for source agencies. We did not quantify the computer costs to source agencies if the computer matching program relied on a decentralized design through which each Administering Entity established separate connections with the source agency or used existing connections. However, we anticipate that the centralized design of the computer matching program achieves economies of scale that result in significant savings to the source agencies.
- *Recipient Agencies (with exception of CMS):* We estimate that the computer (system) costs associated with the computer matching program to recipient agencies (including State-based Marketplaces, Medicaid/CHIP agencies and Basic Health Programs) is \$647 million, versus \$431 million with a manual verification process. We do not require recipient agencies to submit system costs to CMS. This estimate is based on assumptions from CMS operational engagement with these agencies. This cost includes both system and personnel cost, because while a manual process to review and verify consumer information would derive most of its cost from personnel, systems would likely still exist – including a consumer account system and system connections that would be triggered manually; for example accessing the DHS/SAVE system through the manual user interface.
- *CMS:* We estimate the computer (system) costs of maintaining the Data Services Hub that facilitates the computer matching program is \$136.8 million. In contrast, we estimate the computer costs associated with a manual verification process would be \$1.8 billion. This estimate is based on the average cost to process a paper or manual verification today (\$17 per verification) multiplied by the number of eligibility verifications performed on an application times the number of applicants. The number of eligibility verifications depends upon applicants who were not seeking financial assistance (9%) versus those applicants who were seeking financial assistance. We also added an assumption that there would be a 10% reduction of applicants seeking financial assistance with the added burden of a manual verification process.

We note that under this manual process, many of the costs would be transferred from CMS to states. If instead of the current streamlined and centralized computer matching program, CMS required each Administering Entity to establish its own secure connection with TDSs to receive data (or use an existing connection), CMS would still need to establish a secure connection with each TDS for its own use in performing eligibility determinations for the FFM. While the costs of maintaining the Hub would likely be lessened due to the absence of data match requests for Administering Entities, there are economies of scale achieved by allowing the Administering Entities to use the Hub.

Additionally, certain computer costs incurred by the source agencies are transferred to CMS. We estimate these computer costs at \$6.8 million. These costs were not included in the computer costs estimated for source agencies above.

- *Justice Agencies:* We are not aware of any computer costs incurred by justice agencies in connection with this matching program.

### III. BENEFITS

### Key Element 3: Avoidance of Future Improper Payments

#### *To Agencies –*

- *Source agencies:* Source agencies do not receive benefits related to the avoidance of future improper payments, with the exception of CMS, which receives these benefits in its role as a recipient agency (i.e., as the operator of the FFM). These benefits to CMS are described in the recipient agencies section below.
  
- *Recipient agencies:* We believe that our electronic verification sources are a more accurate and efficient means of verifying a consumer’s information compared to both the manual review of consumer-provided documentation and the use of multiple decentralized computer matching programs between each Administering Entity and each TDS. The real-time data matches allowed by the computer matching program increase the efficiency with which we verify a consumer’s information, allowing for increased avoidance of improper payments for the FFM, state-based Marketplaces, Medicaid, CHIP, and Basic Health Programs. For example, real-time capabilities mean the front-end application can be responsive in real time to the consumer input as well as the data received to correct data and/or reduce the need for manual follow-up. Specific examples of this efficiency could include a “prompt” to an applicant to check their social security number if it does not match the first time, allowing a consumer to correct ‘fat finger’ mistakes in seconds rather than go through a lengthy manual process, or requesting specific DHS documentation number follow up information about a consumer who has attested to being a lawful immigrant in a specific category. By increasing the accuracy of our verifications, we (1) avoid improper payments being made to individuals who are ineligible; and (2) reduce the additional time spent by staff at the aforementioned agencies in addressing what appear to be data inconsistencies. Finally, we believe this computer matching program deters fraud and abuse on applications for state health subsidy programs, further avoiding future improper payments. We do not currently have reliable data to quantify these avoided improper payments. As the program matures, we anticipate having data that likely could be used to calculate an approximation of the increased accuracy of online verifications. The Office of Financial Management-led improper payment rate methodology for the Marketplace may be one source of this valuable information.  
We are exploring the possibility of leveraging the computer matching program for use in eligibility determinations for other public benefit programs. If we were to expand the program, we anticipate even more benefits for consumers and the agencies that support such consumer programs.
  
- *Justice Agencies:* We assume that by enabling the FFM and Administering Entities to identify individuals who are ineligible for enrollment in Medicaid, CHIP and Basic Health Programs, or receipt of APTC or CSRs earlier than if a paper-based system was used, the matching program reduces the number and amount of cases referred to the Departments of Justice. At this time we do not have enough information to quantify these benefits.
  
- *To the General Public:* We believe that the use of a centralized, streamlined, electronic computer matching program increases the general public’s confidence in state health

subsidy programs, given a manual process would be laughable given present-day electronic capabilities and the pervasiveness of electronic, real-time processes.

*To Clients:* Data from the computer matching program are used to determine the amount of APTC for which an individual is eligible. Consumers who receive APTC must file an income tax return to reconcile the amount of APTC (based on projected household income) with the final premium tax credit for which the individual is eligible (based on actual household income). Some consumers, particularly those with liquidity constraints, may have trouble repaying improperly paid APTC. The benefit of avoiding improper payments of APTC to these consumers is not quantifiable.

Additional benefits from the matching program to clients are also not quantifiable. By building public confidence in the state health subsidy programs, the computer matching program decreases the stigma of participating in a state health subsidy program.

*Key Element 4: Recovery of Improper Payments and Debts*

Data from the matching program is not currently used to identify and recover improper payments. Annual reconciliation and recovery of improper payments is ultimately performed by the IRS through a process that is also independent from CMS's eligibility activities, including this computer matching agreement. Because data matches under this computer matching program are not used for recovery of improper payments, there are no benefits to estimate in this category. While annual and monthly reporting by Marketplaces to the IRS and consumers is a way of Marketplaces providing data to support IRS's reconciliation, annual and monthly reporting is not an activity covered in the IRS-CMS CMA and therefore is outside the scope of this study. As these uses are not allowed under the CMAs being entered into at this time, there are currently no benefits to quantify in this category for agencies, clients or the general public.

## ATTACHMENT C

### **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 CCIO 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<sup>1</sup> 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.

---

<sup>1</sup> 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	<ul style="list-style-type: none"><li>• <i>Remote:</i> Confirmation via e-mailed link</li></ul>
Level 2	<ul style="list-style-type: none"><li>• <i>Remote:</i> 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.</li><li>• <i>Delegated:</i> Remote or in-person proofing completed by a trusted entity</li></ul>

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<sup>2</sup> 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.

#### *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,

---

<sup>2</sup> 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.

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 help the 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?