

**COMPUTER MATCHING AGREEMENT
 BETWEEN
 THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
 CENTERS FOR MEDICARE & MEDICAID SERVICES
 AND
 THE DEPARTMENT OF DEFENSE
 DEFENSE MANPOWER DATA CENTER
 FOR VERIFICATION OF ELIGIBILITY FOR MINIMUM ESSENTIAL COVERAGE
 UNDER THE PATIENT PROTECTION AND AFFORDABLE CARE ACT THROUGH
 A DEPARTMENT OF DEFENSE HEALTH BENEFITS PLAN**

**CMS Computer Matching Agreement No. 2016-07
 Department of Health and Human Services No. 1602
 DoD-DMDC No. 18**

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

I. PURPOSE, LEGAL AUTHORITIES AND DEFINITIONS

A. Purposes

This Computer Matching Agreement (Agreement) establishes the terms, conditions, and procedures under which the Department of Defense (DoD) will provide information or data (data) to the Centers for Medicare & Medicaid Services (CMS) of the Department of Health and Human Services (HHS).

Under the authority of the 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) and the implementing regulations, CMS, in its capacity as operator of the Federally-facilitated Exchanges (FFE) and the Federal enrollment and eligibility platform, will use DoD's information to verify an Applicant's or Enrollee's eligibility for Minimum Essential Coverage (MEC) through a TRICARE Health Care Program for the purpose of making Eligibility Determinations, including Eligibility Determinations for which HHS is responsible under 45 C.F.R. § 155.302. DoD acknowledges that Administering Entities, which include state-based Exchanges and Basic Health Programs, will use DoD data, accessed through Data Services Hub (Hub), to make Eligibility Determinations.

The Computer Matching and Privacy Protection Act of 1988 (CMPPA) (Public Law 100-503) amended the Privacy Act (5 U.S.C. § 552a) and requires the parties participating in a matching program to execute a written agreement specifying the terms and conditions under which the matching will be conducted. CMS has determined that verifications conducted by

CMS, on behalf of Administering Entities, using the Data Services Hub (Hub), and accessing DoD data will constitute a “computer matching program” as defined in the CMPPA.

The responsible component for CMS is the Center for Consumer Information & Insurance Oversight (CCIIO). CMS will serve as the Recipient Agency, and as such, is responsible for publishing the Federal Register notice required by 5 U.S.C. § 552a(e)(12). The DoD components responsible for the disclosure of is the Defense Manpower Data Center (DMDC). DoD will serve as the Source Agency in this Agreement.

The Defense Manpower Data Center provides the Defense Health Agency (DHA) with the data used to determine medical eligibility, enrollment and medical claims payment via the Defense Enrollment Eligibility Reporting System (DEERS). DHA establishes health care coverage benefits for active duty services members and their family members and retirees and their family members. DMDC, via DEERS, will integrate with the Hub to provide services to verify an Applicant or Enrollee’s eligibility for TRICARE health benefits.

By entering into this Agreement, the Parties agree to comply with the terms and conditions set forth herein and the applicable law and implementing regulations. The terms and conditions of this Agreement will be carried out by authorized officers, employees and contractors of CMS and DoD. The terms and conditions under which state-based Administering Entities may receive and use DoD data will be set forth in a separate agreement between CMS and each state-based Administering Entity.

B. Legal Authorities

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

1. This Agreement is executed pursuant to the Privacy Act of 1974 (5 U.S.C. § 552a) as amended by the CMPPA and the regulations and guidance promulgated thereunder; the Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources” published at 61 Federal Register (Fed. Reg.) 6428 (February 20, 1996), and OMB guidelines pertaining to computer matching published at 54 Fed. Reg. 25818 (June 19, 1989).
2. Under the ACA, certain individuals are eligible for certain financial assistance in paying for private insurance coverage under a Qualified Health Plan (QHP) when enrollment is through an Exchange. Such assistance includes APTCs, under 26 U.S.C. § 36B and section 1412 of the Affordable Care Act, and CSRs under section 1402 of the Affordable Care Act.
3. Section 36B(c)(2) of the Internal Revenue Code of 1986, as added by section 1401 of the ACA, provides that an individual is ineligible for APTC if that individual is eligible for other “minimum essential coverage” (MEC), as defined in 26 U.S.C. § 5000A(f) other than MEC described in 26 U.S.C. § 5000A(f)(1)(C), such as coverage under TRICARE. Section 1402(f) of the ACA provides that an individual is

ineligible for CSRs under §§ 1402(c) and (d)(1) if the individual is not also eligible for the premium tax credit for the relevant month.

4. Section 1331 of the Affordable Care Act authorizes the Basic Health Program (BHP) and Section 1331 (e)(1)(C) requires the state administering BHPs to verify whether an individual is eligible for other Minimum Essential Coverage, such as coverage under TRICARE. 45 C.F.R. § 155.320(d).
5. Section 1411 of the ACA requires the Secretary of HHS to establish a program to determine eligibility for an individual to purchase a Qualified Health Plan (QHP) through an Exchange and to determine eligibility for Insurance Affordability Programs, including APTC and CSR. The system established by HHS under § 1411 to determine eligibility for APTC and CSRs requires an Exchange to verify whether an individual is eligible for other Minimum Essential Coverage, such as coverage through TRICARE, by sending information to HHS for HHS to provide a response. 45 C.F.R. § 155.320(b).
6. Pursuant to section 1411(c)(4)(B) and 1411(d) of the Affordable Care Act, the Secretary of HHS has determined that verification of eligibility for the TRICARE coverage described in this Agreement is best made using a computer matching program as described in this Agreement. An Exchange may use this verification service through the Hub to support Eligibility Determinations for APTCs and CSRs by sending a request to the Hub. CMS facilitates the verification against DoD data, and a response with the result of that verification attempt is sent to the entity that determines eligibility for APTC and CSRs. Under 45 C.F.R. §§ 155.302 and 155.305, the Eligibility Determinations for APTC and CSRs may be made by an Exchange or HHS. CMS carries out the Exchange-related responsibilities of HHS (76 Fed. Reg. 4703 (Jan. 26, 2011)).
7. Under the authority of Sections 1311, 1321, and 1411(a) of the ACA, the Secretary of HHS adopted regulations, 45 C.F.R. § 155.330, which further address the requirements for an Exchange to redetermine eligibility for enrollment in a QHP through an Exchange and for APTC and CSRs during the benefit year based on certain types of changes in circumstances.
8. The Privacy Act, 5 U.S.C. §552a(b)(3), authorizes a Federal agency to disclose information about an individual that is maintained by an agency in an agency system of records (SOR), without the prior written consent of the individual, when such disclosure is pursuant to a routine use. DMDC and CMS have routine uses in their SORs to address their disclosures under this Agreement.
9. Section 1411(f) of the ACA sets forth the appeals authority.
10. Health plans are only permitted to use or disclose protected health information (PHI), such as eligibility and enrollment information, as permitted or required by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Among other

things, the HIPAA Privacy Rule (45 C.F.R. § 164.512(k)(6)) permits a health plan that is a government program providing public benefits, such as TRICARE, to disclose eligibility and enrollment information to an agency administering another government program providing public benefits if the disclosure is required or expressly authorized under regulation or statute. 45 C.F.R. § 155.320(b)(2) expressly authorizes the disclosure to HHS of information regarding eligibility for and enrollment in a health plan, which may be considered PHI, for the purposes of verification of an applicant's eligibility for Minimum Essential Coverage as part of the eligibility determination process for APTC or CSRs.

C. Definitions

For the purposes of this Agreement:

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" means a state Medicaid agency, Children's Health Insurance Program (CHIP), a basic health program (BHP), or an Exchange administering an Insurance Affordability Program;
3. "Applicant" means an individual who is seeking eligibility for him or herself through an application submitted to an Exchange, excluding individuals seeking eligibility for an exemption from the individual shared responsibility payment pursuant to subpart G of Part 155 of title 45 of the Code of Federal Regulations, submitted to a BHP program or transmitted to an Exchange by an agency administering an Insurance Affordability Program for at least one of the following (i) enrollment in a QHP through an Exchange; or (ii) the BHP;
4. "APTC" or "Advanced Premium Tax Credit" has the meaning provided under 45 C.F.R. § 155.20, and means payment of the tax credits specified in section 36B of the Internal Revenue Code (as added by section 1401 of the Affordable Care Act), which are provided on an advance basis to an eligible individual enrolled in a QHP through an Exchange in accordance with sections 1412 of the Affordable Care Act. APTCs are not considered Federal Tax Information under 26 U.S.C. § 6103;
5. "Authorized Representative" means an individual, person or organization acting, in accordance with 45 C.F.R. § 155.227, on behalf of an Applicant or Enrollee in applying for an Eligibility Determination, including a redetermination, and in carrying out other ongoing communications with the Exchange;
6. "Benefit Year" means the calendar year for which a health plan purchased through an Exchange provides coverage for health benefits;
7. "BHP" means Basic Health Program as established under Section 1331 of the Affordable Care Act;
8. "Breach" is defined by 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;
9. "CMS" means the Centers for Medicare & Medicaid Services;
 10. "Cost Sharing Reductions" or "CSRs" is defined at 45 C.F.R. § 155.20 and means reductions in cost sharing for an eligible individual enrolled in a silver level plan in the Exchange or for an individual who is an Indian enrolled in a QHP in the Exchange;
 11. "DEERS" means Defense Enrollment Eligibility Reporting System;
 12. "DHA" means Defense Health Agency;
 13. "DMDC" means the Defense Manpower Data Center;
 14. "DoD" means Department of Defense;
 15. "Eligibility Determination" means the determination of eligibility for Insurance Affordability Programs, including a redetermination based on a self-reported change pursuant to 45 C.F.R. § 155.330, and the process of appealing a decision on a determination when an appeal is provided pursuant to section 1411(f) of the Affordable Care Act;
 16. "Enrollee" means an individual enrolled in a QHP through an Exchange or enrolled in a BHP;
 17. "Exchange" means an American Health Benefit Exchange established under sections 1311(b), 1311(d)(1), and 1321(c)(1) of the ACA, including both State-based Exchanges and FFEs;
 18. "FFE" or "Federally Facilitated Exchange" means an Exchange established by HHS and operated by CMS under Section 1321(c)(1) of the ACA;
 19. "HHS" means the Department of Health and Human Services;
 20. "Hub" or "Data Services Hub" is the, CMS managed, single data exchange for Administering Entities to interface with Federal agency partners. Hub services allow for adherence to Federal and industry standards for security, data transport, data safeguards as well as CMS policy for Administering Entities for Eligibility Determination and enrollment services;
 21. "Insurance Affordability Programs" include (1) a program that makes coverage in a QHP through an Exchange with APTC; (2) a program that makes available coverage in a QHP through an Exchange with CSRs; (3) the Medicaid program established under Title XIX of the Social Security Act; (4) Children's Health Insurance Program (CHIP) established under Title XXI of the Social Security Act; and (5) the Basic Health Program (BHP) established under Section 1331 of the Affordable Care Act;
 22. "MEC" or "Minimum Essential Coverage" is defined in I.R.C. § 5000A(f) and includes health insurance coverage offered in the individual market within a state, which includes a Qualified Health Plan offered through an Exchange, an eligible employer-sponsored plan, or government-sponsored coverage such as coverage under Medicare Part A, TRICARE, or a VHA Health Care Program;
 23. "PII" or "Personally Identifiable Information" is defined by OMB M-07-16 (May 22, 2007) and means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.;

24. "Qualified Health Plan" or "QHP" means a health plan that has in effect a certification that it meets the standards described in subpart C of part 156 in title 45 of C.F.R. issued or recognized by the Exchange through which such plan is offered in accordance with the process described in subpart K of part 155 in title 45 of C.F.R.;
25. "Recipient Agency" is defined by the Privacy Act (5 U.S.C. § 552a(a)(9)) and means any agency, or contractor thereof, receiving records contained in a System of Records from a Source Agency for use in a matching program. As the Recipient Agency, CMS is responsible for publishing the Federal Register notice required by 5 U.S.C. § 552a(e)(12);
26. "Security Incident" means the act of violating an explicit or implied security policy, which includes attempts (either 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;
27. "Source Agency" is defined by the Privacy Act (5 U.S.C. § 552a(a)(11)), means any agency that discloses Records contained in a System of Records to be used in a matching program. The DoD is the Source Agency in this Agreement;
28. "State-based Exchange" means an Exchange established and operated by a State, and approved by HHS under 45 C.F.R. § 155.105;
29. "System of Records" is defined by the Privacy Act (5 U.S.C. § 552a(a)(5)), means a group of any Records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual; and
30. "TRICARE" means a DoD government sponsored health program which establishes health care coverage benefits for active duty services members and their family members, retirees and their family members.

II. RESPONSIBILITIES OF THE PARTIES

A. CMS Responsibilities

1. CMS will develop procedures through which an Applicant or Enrollee may request an Eligibility Determination via a single, streamlined application.
2. CMS will develop procedures through which an Administering Entity can request information from and match an Applicant's or Enrollee's information with DoD's, DEERS system of records through the CMS Hub. CMS will only request data from or request a data match with DoD's records when necessary to make an Eligibility Determination, including an initial determination of eligibility, a determination based on a self-reported change, or a re-verification at the end of the inconsistency period.
3. CMS will receive the DoD response data elements through the Hub and will utilize the information provided by DoD in making Eligibility Determinations.

4. CMS will develop procedures through which a state-based Administering Entity can request information from DoD through the Hub to make Eligibility Determinations.
5. CMS will provide Congress and the OMB with notice of this matching program and will publish the required matching notice in the Federal Register.
6. CMS will enter into agreements with state-based Administering Entities that bind these entities, including employees, contractors, and agents, to comply with the privacy and security standards and protections for PII, including requirements for these entities and their employees, contractors, and agents to comply with the use and disclosure limitations set forth in section 1411(g) of the ACA, and privacy and security standards that are consistent with the principles outlined under 45 C.F.R. § 155.260, and privacy and security standards that are consistent with the terms and conditions of this Agreement.
7. CMS will ensure the receipt of appropriate consents from Applicants or Enrollees for use of PII collected, used, and disclosed for the purposes and programs outlined in this Agreement.

B. DoD Responsibilities

1. DoD will develop procedures to respond to verification requests by CMS to transmit information from DEERS to verify or validate eligibility for TRICARE health benefit programs.
2. DoD will perform deterministic data matching to match the identity of the Applicant or Enrollee's inputs with DoD data records.
3. DoD will provide its data to the Hub, in accordance with Section IV. B. 2. in order to verify whether the Applicant or Enrollee was eligible for DoD TRICARE benefit programs within the period requested by CMS.

III. JUSTIFICATION AND ANTICIPATED RESULTS

A. Justification

Under the ACA, certain individuals are eligible to purchase health insurance coverage from an Exchange and for assistance in paying for the premiums and cost sharing related to that coverage in the form of APTC and CSRs. Pursuant to 26 U.S.C. § 36B(c)(2) and § 1402(f)(2) of the ACA, an individual generally may not be found eligible for APTC and CSRs for any month during which the applicant is eligible for MEC other than coverage described in section 5000A(f)(1)(C) (relating to coverage in the individual market). Under section 1331(e)(1)(C) of the Affordable Care Act, individuals are eligible for enrollment in a Basic Health Program if they are not eligible for MEC other than coverage described in section 5000A(f)(1)(C) (relating to coverage in the individual market). The coverage provided through TRICARE generally qualifies as MEC which

may disqualify an individual from receiving APTC and CSRs, and enrolling in a Basic Health Program.

The Affordable Care Act requires the use of a single, streamlined application which may be used to apply for eligibility for enrollment in an Insurance Affordability Program (e.g., APTC, CSRs). An Applicant must be able to file this application online, by telephone, in person or by mail with any of the entities administering these programs. The ability for an Applicant or Enrollee to access the appropriate coverage and financial assistance across multiple programs through a single streamlined application and coordinated eligibility process means that no matter how an application is submitted or which program receives the application data, an Applicant or Enrollee will experience a consistent process and receive an appropriate Eligibility Determination, without the need to submit information to multiple programs.

In order to provide accurate and efficient Eligibility Determinations when an Applicant or Enrollee uses this single streamlined application and coordinated eligibility process, a computer matching program is necessary because it provides an efficient and prompt means to verify whether one of the criteria for eligibility for APTCs, CSRs, and the Basic Health Program is met. Specifically, an Applicant or Enrollee cannot be eligible for enrollment in health coverage under TRICARE and qualify for APTC, CSRs, or a Basic Health Program.

B. Anticipated Results

CMS anticipates that this data transfer will produce expedited Eligibility Determinations and will minimize administrative burdens. The benefit of this data match with respect to the Insurance Affordability Programs is the increased assurance that CMS achieves efficiencies and administrative cost savings. This collaborative model, which offers service-based access to authoritative data, will lessen financial and administrative burdens by eliminating the need for each State to execute several agreements with multiple federal agencies.

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

A. Systems of Records

1. The CMS System of Records (SOR) that supports this data matching program is the Health Insurance Exchanges Program (HIX), CMS System No. 09-70-0560, as amended, first published at 78 Federal Register, 8538, February 6, 2013, located at the Terremark data center, in Culpeper, Virginia. Routine Use 3 supports CMS' disclosure to DoD.
2. DoD maintains the following SOR with the identified routine use to support this data matching program:
 - a. Defense Enrollment Eligibility Reporting Systems (DEERS), DoD System No. DMDC 02 DoD, published November 04, 2015, 80 FR 68304, located at the DISA DECC Columbus in Columbus, OH. Routine Use 6f supports DoD's disclosure to CMS.

B. Specified Data Elements

1. From CMS to DoD. For each Applicant or Enrollee seeking an Eligibility Determination, the Administering Entity will submit a request through CMS by way of the Hub to DMDC that may contain, but is not limited to, the following specified data elements in a fixed record format:
 - a. Transaction ID
 - b. Social Security Number (SSN)
 - c. Input First Name
 - d. Input Middle Name
 - e. Input Surname
 - f. Input Date of Birth
 - g. Input Gender
 - h. Input Requested QHP coverage effective date
 - i. Input Requested QHP coverage end date
2. From DoD to CMS. For each Applicant or Enrollee seeking an Eligibility Determination through an Administering Entity, DMDC will provide to the Hub one of several outputs indicating whether an individual has MEC or not. The response will be in a standard fixed record electronic format (e.g., response file) and may contain, but is not limited to, the following specified data elements:
 - a. Insurance End Date

- b. Person SSN Identification
- c. Response Code
- d. Response Code Text

C. Number of Records

The following table provides the base estimates for the total number of transactions in FY 2016 and FY 2017, as well as the number of transactions in the estimated highest month within each of those years. These estimates are subject to change as business assumptions or estimates are updated and/or refined.

	FY 2016 Total	FY 2016 Highest Month	FY 2017 Total	FY 2017 Highest Month
Base Estimate	90,794,949	10,115,822	114,473,371	12,587,959

V. PROCEDURES FOR INDIVIDUAL NOTICE

- A. CMS will publish notice of the matching program in the Federal Register as required by the Privacy Act (5 U.S.C. § 552a (e)(12)).
- B. At the time of application or when an individual reports a change of circumstances, an Administering Entity will provide a notice to Applicants or Enrollees on the streamlined eligibility application that the information they provide may be verified with information in the records of other Federal agencies. The Administering Entity will ensure provision of a redetermination notice in accordance with applicable law.

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. Verification and Opportunity to Contest Procedures

When an Exchange determines that an individual is ineligible for APTC or CSRs based on the information provided by the match, the Exchange will comply with 45 C.F.R. §155.315(f). Before an Exchange may take any adverse action based on the information received from the match, the individual will be permitted to provide the necessary information or documentation to verify eligibility information pursuant to 45 C.F.R. §155.315(f)(1). In addition, the Exchange will notify the individual and provide the information as required under 45 C.F.R. §155.315(f)(2).

VII. ACCURACY ASSESSMENTS

DMDC currently estimates that information within DEERS is 99% accurate.

VIII. PROCEDURES FOR RETENTION AND TIMELY DESTRUCTION OF IDENTIFIABLE RECORDS

DoD and CMS will retain data received from the other party via the Hub only for the period of time required to verify an Applicant or Enrollee's eligibility for TRICARE health benefits under this matching program and will then destroy the data by electronic purging, unless DoD or CMS are required to retain the information for enrollment, billing, payment, program audit purposes, or legal evidentiary purposes or where they are required by law to retain the information. The CMS FFE and state-based Administering Entities will retain data for such purposes and under the same terms. In case of such retention, DoD and CMS will retire the retained data in accordance with the applicable Federal Records Retention Schedule (see 44 U.S.C. § 3303a). DoD and CMS will not create permanent files or a separate system comprised solely of the data provided by the other party.

IX. SECURITY PROCEDURES

- A. General: CMS and DoD will maintain a level of security that is commensurate with the risk and magnitude of harm that could result from the loss, misuse, disclosure, or modification of the information contained on the system with the highest appropriate sensitivity level.
- B. Legal Compliance: CMS and DoD shall comply with the limitations on use, disclosure, storage, transport, and safeguarding of data under all applicable Federal laws and regulations. These laws and regulations include section 1411(g) of the Affordable Care Act; the Privacy Act of 1974; the E-Government Act of 2002, which includes the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §§ 3541-3549, as amended by the Federal Information Security Modernization Act, 44 U.S.C. §§ 3551-3558; HIPAA; the Computer Fraud and Abuse Act of 1986; the Clinger-Cohen Act of 1996; and the corresponding implementation regulations for each statute. Additionally, CMS will follow Federal, HHS, and CMS policies including the HHS Information Security and Privacy Policy, as amended, and the CMS Information Security Acceptable Risk Safeguards (ARS) and CMS Minimum Security Requirements.

CMS and DoD will comply with OMB circulars and memoranda, such as Circular A-130, revised, Management of Federal Information Resources (November 28, 2000), and Memorandum M-06-16, Protection of Sensitive Agency Information (June 23, 2006); National Institute of Standards and Technology (NIST) directives and publications; and the Federal Acquisition Regulations. These laws, directives, and regulations include requirements for safeguarding Federal information systems and PII used in Federal agency business processes, as well as related reporting requirements. The Parties

recognize and will implement the laws, regulations, NIST standards, and OMB directives including those published subsequent to the effective date of this Agreement.

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

- C. Loss, Potential Loss, Incident Reporting, and Breach Notification: CMS and DoD will comply with OMB reporting guidelines in the event of a loss, potential loss, Security Incident or Breach of PII (see OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006); OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007); and OMB M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices (Oct. 3, 2014). The Party experiencing the incident will notify the other agency's System Security Contact named in this Agreement within one (1) hour of discovering the loss, potential loss, Security Incident, or Breach. If the Party experiencing the loss, potential loss, Security Incident, or Breach is unable to speak with the other Party's System Security Contact within one (1) hour or if for some reason contacting the System Security Contact is not practicable (e.g. outside of normal business hours), then the following contact information will be used:

- DMDC Privacy Office: dodhra.dodc-mb.dmdc.list.privacy-office@mail.mil
- CMS IT Service Desk: 1-(800) 562-1963 or e-mail
- [CMS IT Service Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov)

The Party that experienced the loss, potential loss, Security Incident, or Breach will be responsible for following its established procedures, including notifying the proper organizations (e.g., United State Computer Emergency Readiness Team (US-CERT)), conducting a breach and risk analysis, and making a determination of the need for notice and/or remediation to individuals affected by the loss.

Parties under this agreement will follow PII breach notification policies and related procedures as required by OMB guidelines and the US-CERT Federal Incident Notification Guidelines. If the Party experiencing the breach determines that the risk of harm requires notification to the affected individuals or other remedies that Party will carry out these remedies without cost to the other Party.

- D. Administrative Safeguards: CMS and DoD will restrict access to the matched data and to any data created by the match to only those authorized users of the Hub, e.g., Administering Entities and their employees, agents, officials, contractors, etc., who need it to perform their official duties in connection with the uses of data authorized in this Agreement. Further, CMS and DoD will advise all personnel who will have access to the data matched and to any data created by the match of the confidential nature of the data,

the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable Federal laws.

- E. Physical Safeguards: CMS and DoD will store the data matched and any data created by the match in an area that is physically and technologically secure from access by unauthorized persons at all times. Physical safeguards may include, but are not limited to, door locks, card keys, biometric identifiers, etc. Only authorized personnel will transport the data matched and any data created by the match. CMS and DoD will establish appropriate safeguards for such data, as determined by a risk-based assessment of the circumstances involved.
- F. Technical Safeguards: CMS and DoD will process the data matched and any data created by the match 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. Systems personnel must enter personal identification numbers when accessing data on a party's systems. DoD and CMS will strictly limit authorization to those electronic data areas necessary for the authorized analyst to perform his or her official duties.
- G. Application of Policies and Procedures: The Parties will adopt policies and procedures to ensure that each party uses the information described in this Agreement that is contained in their respective records or obtained from each other solely as provided in this Agreement. CMS and DoD will comply with their respective policies and procedures and any subsequent revisions.
- H. On-Site Inspections: Each party has the right to monitor the other party's compliance with FISMA and OMB M-06-16 requirements for data exchanged under this Agreement, and to audit compliance with this Agreement, if necessary, during the lifetime of this Agreement, or any extension of this Agreement. Each party will provide the other party with any reports and/or documentation relating to such inspections at the other party's request. Each party may request an on-site inspection in addition to requesting reports and/or documentation.
- I. Compliance. CMS must ensure information systems and data exchanged under this matching agreement are maintained compliant with CMS guidance CMS Acceptable Risk Safeguards and Minimum Acceptable Risk Standards for Exchanges –(MARS-E) Exchange Reference Architecture Supplement. The MARS-E suite of documents can be found at: <http://www.cms.gov/ccio/resources/regulations-and-guidance/index.html>, under Minimum Acceptable Risk Standards. To the extent, these documents are revised during the term of this Agreement, CMS must ensure compliance with the revised version.

X. RECORDS USAGE, DUPLICATION AND DISCLOSURE

CMS and DoD will comply with the following limitations on use, duplication, and disclosure of the electronic files and data provided by the other party under this Agreement:

- A. CMS and DoD will only use or disclose the data for the purposes described in this Agreement or allowed by applicable SORNs or Federal law.
- B. The matching data provided by DoD under this Agreement will remain the property of DoD and will be retained by CMS and Administering Entities to be used for audits to verify the accuracy of matches and to adjudicate appeals.
- C. CMS will restrict access to data solely to officers, employees, contractors of CMS and Administering Entities, their officers, employees, and contractors. Through the Hub CMS may disclose the data received under this Agreement to Administering Entities pursuant to separate Computer Matching Agreements that authorize such entities to use the data for Eligibility Determinations regarding APTC, CSRs, and BHP.
- D. CMS FFE and Administering Entities will restrict access to the results of the data match to Applicants and Enrollees, application filers, and Authorized Representatives of such persons; and to individuals or entities who have been authorized by CMS and are bound by regulation or are under agreement with CMS or an Administering Entity to assist with Eligibility Determinations and enrollment.

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 DMDC records, as necessary, in order to verify compliance with this Agreement.

XII. REPORT TO CONGRESS AND OMB

When both the HHS Data Integrity Board (DIB) and the DoD 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 DoD.

XIII. REIMBURSEMENT

Expenses incurred by this data match will not involve any payments or reimbursement between DoD and CMS. Cost adjustments, however, may be made in the future between the parties. DoD and CMS may make such adjustments by means of a reimbursable agreement between the parties.

XIV. PERSONS TO CONTACT

A. The DoD contacts are:

1. Project Coordinator

Brian Stroud
Defense Enrollment Eligibility Reporting System
Defense Manpower Data Center
831.583.2500 ext 5575
Email: Brian.K.Stroud4.civ@mail.mil

2. Privacy Issues

Samuel M. Peterson
Privacy/FOIA Branch Chief
DMDC
(831) 583-2400 x4457
Email: Samuel.M.Peterson2.civ@mail.mil

Tori Rodrigues
Privacy Analyst
DMDC PM Support
(831) 583-2400 x4270
Email: Victoria.W.Rodrigues.ctr@mail.mil

3. Security Issues

Vickie Galante, CISSP
Information Assurance Officer
(831) 583-2400 x5447
Victoria.J.Galante.civ@mail.mil

B. The CMS contacts are:

1. Program Issues:

Elizabeth Kane
Acting Director, Verifications Policy and Operations Division
Eligibility and Enrollment Policy and Operations Group
Center for Consumer Information and Insurance Oversight
Centers for Medicaid and Medicare Services
Phone: (301) 492-4418
E-Mail: Elizabeth.Kane@cms.hhs.gov

2. 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

3. Privacy and Agreement Issues:

Walter Stone
CMS Privacy Officer
Division of Information Security, Privacy Policy & Governance
Offices of Enterprise Management
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Mail Stop: N1-24-08
Baltimore, MD 21244-1849
Telephone: 410-786-5357
Fax: 410-786-1347
E-mail: walter.stone@cms.hhs.gov

4. 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

5. 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

XV. DURATION, MODIFICATION, AND TERMINATION

- A. **Effective Date:** The Effective Date of this Agreement is April 2, 2016 provided that the following notice periods have lapsed: thirty (30) days from the date CMS publishes a Computer Matching Notice in the Federal Register; forty (40) days from the date of the matching program notice that is sent to the Congressional committees of jurisdiction under 5 U.S.C. § 552a(o)(2)(A); and forty (40) days from the date of the matching program notice that is sent to OMB. If such notice periods have not lapsed on or before April 2, 2016, the Effective Date of this Agreement will be the first day after such notice periods have lapsed.
- B. **Term:** The initial term of this Agreement will be eighteen (18) months.
- C. **Renewal:** The DIBs of HHS and DoD 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 DoD can certify the following to their DIBs:
1. The matching program will be conducted without change; and
 2. The parties have conducted the matching program in compliance with the original agreement.
 3. 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.
- 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 DIBs of HHS and DoD.
- E. **Termination:** This Agreement may be terminated at any time upon the mutual written consent of the parties. Either party may unilaterally terminate this Agreement upon written notice to the other party, in which case the termination will be effective ninety (90) days after the date of the notice, or at a later date specified in the notice.

XVI. LIABILITY

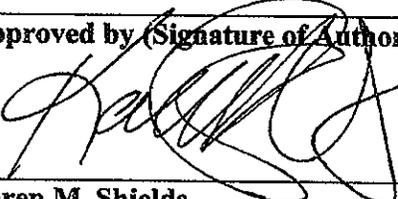
- A. Each party to this Agreement shall be liable for acts and omissions of its own employees.
- B. Neither party shall be liable for any injury to another party's personnel or damage to another party's property, unless such injury or damage is compensable under the Federal Tort Claims Act (28 U.S.C. § 1346(b)), or pursuant to other Federal statutory authority.
- C. Neither party shall be responsible for any financial loss incurred by the other, whether directly or indirectly, through the use of any data furnished pursuant to this Agreement.

XVII. INTEGRATION CLAUSE

This Agreement constitutes the entire agreement of the parties with respect to its subject matter and supersedes all other data exchange agreements between the Parties that pertain to the disclosure of data between DoD and CMS for the purposes described in this Agreement. The parties have made no representations, warranties, or promises outside of this Agreement. This Agreement takes precedence over any other documents that may be in conflict with it.

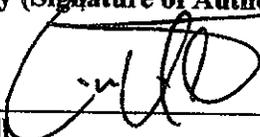
XVIII. APPROVALS**A. Centers for Medicare & Medicaid Services Program Official**

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 their respective organization to the terms of this Agreement.

Approved by (Signature of Authorized CMS Program Official) 	
Karen M. Shields Deputy Center and Operations Director Center for Consumer Information & Insurance Oversight Centers for Medicare & Medicaid Services	Date: 2-2-18

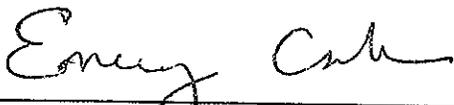
B. Centers for Medicare & Medicaid Services Approving Official

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

Approved by (Signature of Authorized CMS Program Official) 	
Timothy Hill Deputy Director Centers for Medicaid and CHIP Services Centers for Medicare & Medicaid Services	Date: 2/2/2016

C. Centers for Medicare & Medicaid Services Approving 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 their respective organization to the terms of this Agreement.

Approved by (Signature of Authorized CMS Approving Official)	
	
Emery J. Csulak, Director Information Security and Privacy Group, and Senior Official for Privacy Offices of Enterprise Management Centers for Medicare & Medicaid Services	Date: 2-3-16

D. Data Integrity Board: Department of Health and Human Services

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

Approved by (Signature of Authorized HHS DIB Official)	
	
Colleen Barros Chairperson, HHS Data Integrity Board Acting Assistant Secretary for Administration U.S. Department of Health and Human Services	Date: 3/1/10

E. DMDC 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 their respective organization to the terms of this Agreement.

Approved By (Signature of Authorized DMDC Approving Official)	
SNAVELY- DIXON.MARY.M.1116074377	Digitally signed by SNAVELY-DIXON.MARY.M.1116074377 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA, cn=SNAVELY-DIXON.MARY.M.1116074377 Date: 2016.02.04 13:28:57 -05'00'
Mary Snavely-Dixon Director Defense Manpower Data Center	Date:

F. DIB: Department of Defense

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

Approved By (Signature of Authorized DoD DIB Official)	
	
Joo Y. Chung Chair Defense Data Integrity Board Department of Defense	Date: 3/10/16

Attachment A: Proposed Federal Register Notice

Attachment B: Proposed Master Cost Benefit Analysis (CBA)