COMPUTER MATCHING AGREEMENT
BETWEEN THE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
Centers for Medicare & Medicaid Services
AND THE
DEPARTMENT OF TREASURY
BUREAU OF THE FISCAL SERVICE

CMS Computer Match No. 2014-04
HHS Computer Match No. 1402

I. PURPOSE, LEGAL AUTHORITY, AND DEFINITIONS

A. Purpose

The purpose of this Computer Matching Agreement (CMA) is to establish the conditions, safeguards, and procedures under which the Centers for Medicare & Medicaid Services (CMS) will conduct a computer matching program with the Department of Treasury Bureau of the Fiscal Service (Fiscal Service) to provide identifying information, through Treasury's Working System. The information will be used by CMS to detect suspected instances of programmatic fraud, waste, and abuse (FW&A). Using a computer matching program for this purpose provides prompt access to up-to-date information, and avoids the need to manually compare files.

Pursuant to the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA) and Office of Management and Budget (OMB) Memorandum (M) 13-20, this matching agreement covers a Do Not Pay matching program conducted for the purposes of the Do Not Pay Initiative and involves the recipient agency, CMS, being provided with results from an automated comparison between CMS Systems of Records and one or more of the Privacy Act databases contained within Treasury's Working System.

CMS is designated as the recipient agency as defined by the Privacy Act (5 U.S.C. §552a (a) (9)), the agency receiving the records for use in this matching program. As the recipient agency, CMS is responsible for publishing the *Federal Register* notice required by 5 U.S.C. 552a (e) (12). Fiscal Service is designated as the source agency as defined by the Privacy Act at 5 U.S.C. §552a (a) (11), the agency disclosing its records, for use in this matching program.

B. Legal Authority

1. This matching agreement between Fiscal Service and CMS is executed pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, the OMB Circular A-130 entitled, Management of Federal Information Resources, at 61 Federal Register (Fed. Reg.) 6428-6435 (February 20, 1996), and OMB guidelines pertaining to computer matching at 54 Fed. Reg. 25818 (June 19, 1989) and 56 Fed. Reg. 18599 (April 23, 1991); and the computer matching portions of Appendix I to OMB Circular No. A-130 as amended at 61 Fed. Reg. 6428, February 20, 1996;

2. The Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA), 31 U.S.C. 3321 (note), Pub. L. 112-248.
3. OMB M-13-20 (Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative);
4. Memorandum on Enhancing Payment Accuracy through a "Do Not Pay List" June 18, 2010;
5. Executive Order 13520 "Reducing Improper Payments" (November 20, 2009);
6. The Improper Payment Elimination and Recovery Act of 2010, Pub.L.111-204; and
7. The Improper Payments Information Act of 2002, 31 U.S.C. 3321 (note), Pub.L. 107-300.

C. Definitions

1. **"CMS"** means the Centers for Medicare & Medicaid Services.
2. "**CMA**" or "**matching agreement**" means Computer Matching Agreement as defined by the Privacy Act (5 U.S.C. §552a (o)).
3. "**DIB**" means Data Integrity Boards of the respective agencies participating in the match.
4. "**M-13-20**" means OMB Memorandum 13-20 (Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative) which provides guiding principles and requirements for this matching program.
5. "**Do Not Pay Initiative"** means the initiative codified by section 5 of IPERIA to facilitate Federal agencies' review of payment or award eligibility for purposes of identifying and preventing improper payments. The initiative may include other activities, as designated by OMB[1].
6. "**Treasury's Working System"** means the Do Not Pay Initiative functions performed by the Department of the Treasury that are authorized by section 5(a)(2) of IPERIA and section 5(b) of M-13-20. Treasury's Working System includes Treasury's Privacy Act system of records for Do Not Pay Initiative activities, including other activities such as investigation activities for fraud and systemic improper payments detection through analytic technologies and other techniques.
7. "**Do Not Pay matching program**" means a matching program that is conducted for purposes of the Do Not Pay Initiative and involves at least one of the databases enumerated in section 5(a)(2) of IPERIA and/or a database designated by OMB pursuant to section 5(b) of M-13-20. Do Not Pay matching programs are subject to alternative standards and procedures (as provided in M-13-20) that are different from the standards and procedures that apply to matching programs outside of the Do Not Pay Initiative.
8. **Original source agency"** means a Federal agency that discloses records from a system of records to another agency in order to allow that agency to use the records in a matching program with a payment-issuing agency. For the purposes of a Do Not Pay matching program involving Treasury's Working System, an original source

[1] Section 3 of OMB Memorandum M-13-20 (Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative)

agency discloses records to Treasury in order to allow Treasury to engage in a Do Not Pay matching program with payment-issuing agencies. In a Do Not Pay matching program, original source agencies need not be a party to a matching agreement between Treasury and a payment-issuing agency.

9. **"Parties"** means a collective reference to CMS and Fiscal Service.
10. **"Payment-issuing agency"** means a Federal agency that has the authority to issue a payment or award and engages in a matching program for the purposes of determining or verifying eligibility for the payment or award under a Federal benefit program or of recouping the payment under a Federal benefit program. Generally, the payment-issuing agency will be the agency that benefits from the matching program. The payment-issuing agency is responsible for conducting the cost-benefit analysis and meeting the reporting and publication requirements in the matching provisions of the Privacy Act. If more than one payment-issuing agency is a party to a matching program, the payment-issuing agencies may assign these responsibilities as described in section 12(c) of M-13-20.[2]

II. RESPONSIBILITIES OF THE PARTIES

A. CMS will:

1. Coordinate with Fiscal Service to gain access to services provided through Treasury's Working System, which execute the matching activities for which this Do Not Pay matching program requires.
2. Only invoke services that produce outputs under this agreement when necessary to make a payment determination.
3. Provide the required data elements necessary and agreed upon by the Parties in support of obtaining match results from Treasury's Working System, including, but not limited to, First and Last Name, Date of Birth, and Social Security Number (SSN).
4. Receive the results derived from matches between the systems of records outlined in this agreement and utilize the results provided in making payment determinations.
5. Advise Fiscal Service when errors in payment-issuing agency data are identified and follow established processes to log and correct data to promote data accuracy in Treasury's Working System, while ensuring fairness to the individual or entity record subject.
6. Provide Congress and the OMB with notice of this matching program and will publish the required matching notice in the Federal Register.

B. Fiscal Service will:

1. Execute the matching activities between the system(s) of records listed in this matching agreement and provide detailed results through Treasury's Working System, contingent on the original source agency making its data refresh available timely, accurate, and complete.

[2] For guidance on the publication and reporting requirements of the Privacy Act, see OMB Circular A-130, Appendix I

2. Provide matching results to CMS, on a non-reimbursable basis, to support CMS in identifying, preventing or recouping improper payments.
3. Notify CMS when errors in the original source data are identified, and follow established processes to log and correct data in order to promote data accuracy in Treasury's Working System while ensuring fairness to the individual or entity record subject.

III. JUSTIFICATION AND ANTICIPATED RESULTS

A. Justification

The parties to this agreement have determined that a computer matching program is the most efficient, expeditious, and effective means of obtaining and processing the information needed to identify individuals who may be ineligible for certain payments and benefits. The principal alternative to using a computer matching program for identifying such individuals would be to conduct a manual comparison of all files regarding an individual or entity seeking payment or other benefit from a Federal agency. Conducting a manual match, however, would clearly impose a considerable administrative burden and would result in additional delay in the eventual recovery of any outstanding debts. By contrast, when using a computer matching program, information on successful matches (hits) can be provided within real-time of receipt of the request for payment.

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 CMS fraud and abuse program is the increased assurance that CMS achieves efficiencies and administrative cost savings to CMS payment, procurement, and benefit programs. This collaborative model, which offers service-based access to authoritative data, will lessen financial and administrative burdens by eliminating the need for individual CMS payment, procurement, and benefit programs to execute several Memoranda of Agreement with multiple Federal agencies.

Fiscal Service does not receive any direct benefit as a result of this matching program.

C. Waiver of Cost Benefit Analysis

In fiscal year (FY) 2011, CMS documented savings of approximately $600 million in recovery of mistaken payments and denial of claims in Medicare Secondary Payer (MSP) situations identified through the MSP matching program. The total cost of the data match activities for the MSP matching program was approximately $3.5 million. The benefit to cost ratio was approximately 171:1. CMS predicts a similar benefit to the cost ratio for each of the anticipated uses of the Do Not Pay Initiative covered by this agreement and that the potential savings of the anticipated uses or programs, including efforts to detect suspected instances of programmatic fraud, waste and abuse, will produce a similar result.

IV. DESCRIPTION OF RECORDS TO BE MATCHED

The parties to this agreement must publish a system notice ("system of records notice" or "SORN") pursuant to subsection (e)(4) of the Privacy Act containing "routine uses" established pursuant to subsection (b) (3) of the Privacy Act for each system of records from which they intend to disclose Privacy Act protected information.

A. System of Records Maintained by Fiscal Service

Fiscal Service will provide CMS with information extracted from Fiscal Service's Treasury/Fiscal Service .023 System of Records, which maintains original source agency data relevant to this Do Not Pay matching program. Routine use A allows the Fiscal Service to disclose information to assist CMS in identifying, preventing or recouping improper payments. A copy of the SORN is given as Attachment 1.

B. Systems of Record Maintained by CMS

The matching program will be conducted with data maintained by CMS in the Provider Enrollment, Chain, and Ownership System (PECOS), System No. 09–70–0532, established at 66 Fed. Reg., 51961 (October 11, 2001). PECOS routine use number 2 will allow PECOS data to be disclosed to Fiscal Service to assist Fiscal Service in contributing to the accuracy of CMS Medicare benefit payments. PECOS routine use number 1 will allow results from this Do Not Pay matching program to be disclosed to CMS contractors, consultants, and grantees that assist CMS with PECOS purposes. A copy of the SORN is given as Attachment 2.

C. Number of Records

Through this Do Not Pay matching program, Fiscal Service will provide CMS the result of automated matches resulting from this matching agreement. Record count of Treasury's Working System supporting this agreement amounts to approximately 9.2 million records of individuals and companies maintained in its Treasury/Fiscal Service .023 System of Records. CMS will provide files containing approximately 5.4 million individuals and entities in the PECOS database system for matching against Treasury's Working System.

D. Specified Data Elements

See Attachment 3 for the original source agency data elements used in this match.

E. The Effective Date of This Agreement

The effective date of this agreement and the date when the matching program may begin shall be at the expiration of the 30-day public comment period following CMS's publication pursuant to 5 U.S.C. § 552a (e)(12) of notice of this matching program in the Fed. Reg., or the 40-day OMB review period provided for in Circular A-130 or 30- days after copies of the agreement are transmitted to Congress, whichever date is latest.

V. NOTICE PROCEDURES

Fiscal Service will provide notice of the computer matching program via http://donotpay.treas.gov.

Procedures for providing individualized notice at the time of application and notice periodically thereafter is directed by CMS' DIB. Any deficiencies as to direct notice to the individual for the matching program are mitigated by the indirect or constructive notice that is afforded the individual by agency publication in the Federal Register of both the (1) applicable routine use notice, as required by subsection (e)(11) of the Privacy Act; and (2) the proposed Federal Register match notice, as required by subsection (e)(12) of the Privacy Act, announcing the Agency's intent to conduct computer matching programs designed to give critical information to paying agencies to help reduce improper payments. This matching program for the purposes of the DNP Initiative is initiated in accordance with IPERIA and M-13-20 which further support agencies to reduce improper payments.

VI. VERIFICATION PROCEDURES, AND OPPORTUNITY TO CONTEST

A. Verification of Match Information

1. CMS will take appropriate steps to independently verify all information received from Treasury's Working System to determine the validity and/or applicability of the information obtained through this matching program prior to the termination, denial, suspension or reduction of any benefits.
2. The parties agree that the occurrence of a match is not conclusive evidence that the individual who or organization that is the subject of the search and the individual or the subject in the search results are the same person or organization.
3. CMS is responsible for verifying and determining whether the search results retrieved from Treasury's Working System are consistent with the information in their files and for resolving any discrepancies or inconsistencies as to positive identification on an individual basis.
4. CMS will screen the initial data to verify that the matched individual or organization is in fact the payment/benefit recipient about which/whom the search was initiated. CMS will do this by separately comparing the "match results" file with the information in their files to verify the individual's or organization's identity and will conduct independent inquiries to resolve questionable identities.
5. Any discrepancies or inconsistencies in the original source agency data files, based on information received from Treasury's Working System, or developed as a result of the match, will be independently investigated and verified by CMS prior to taking any adverse action against any individual or organization.

B. Opportunity to Contest

1. If CMS has verified the adverse information, CMS shall provide the individual with notice and an opportunity to contest before taking adverse action. The notice shall inform the individual of the relevant information and give the individual an opportunity to provide an explanation.
2. Individuals shall have 30 days to respond to a notice of adverse action, unless a statute or regulation provides a different period of time. For additional guidance on notice and opportunity to contest, agencies shall consult Final Guidance Interpreting the Provisions of Public Law I 00-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818, 25827 (June 19, 1989).

VII. DISPOSITION OF MATCHED ITEMS

A. CMS acknowledges and agrees to:

1. Maintain all identifiable records received from Fiscal Service in accordance with Privacy Act of 1974 (5 U.S.C. 552a), as amended, (Public Law (Pub. L.) 100-503, the Computer Matching and Privacy Protection Act (CMPPA) of 1988), and the Office of Management and Budget (OMB) Circular A-130 entitled, Management of Federal Information Resources.
2. Not create a separate file or system of records that consists of information concerning only those individuals who are involved in this specific matching program except as is necessary in controlling and/or verifying the information for purpose of this program.
3. Destroy the matching results file generated through this matching operation as soon as the information has served the matching program's purpose and all legal retention requirements established in conjunction with the National Archives and Records Administration (NARA), and M-13-20, under applicable procedures have been met.

VIII. SAFEGUARD PROCEDURES

A. Both CMS and Fiscal Service will comply with the requirements of the Federal Information Security Management Act (FISMA) (PL 107-347, title Ill, section 301) and OMB M-06-16 (Protection of Sensitive Agency Information) as it applies to the electronic storage and transport of Personally Identifiable Information (PII) between agencies and the internal processing of records received under the terms of this agreement.

B. CMS will protect Fiscal Service's information in accordance with published OMB computer matching guidelines and applicable Privacy Act provisions. Any additional internal security procedures and policies in place supporting the protection of individual privacy by CMS are incorporated in this agreement. Match result records obtained by CMS through the use of Treasury’s Working System services shall be handled in such a manner that restricts access to the data, so the data is accessed only by those individuals authorized to review the data to accomplish the purpose outlined in this agreement. Criminal penalties for willful unlawful disclosure pursuant to the Privacy Act shall be made known to those authorized access to this data through Treasury’s Working System.

IX. RECORDS USAGE DUPLICATION AND DISCLOSURE RESTRICTIONS

A. CMS acknowledges and agrees that:

1. Records provided to Fiscal Service by original source agencies remain the property of the original source agency and it is only pursuant to IPERIA and M-13-20 that Fiscal Service maintains original source agency records within Treasury/Fiscal Service .023 system of records to carry out Do Not Pay matching program activities.
2. Records provided by Fiscal Service will not be used to extract information concerning individuals therein for any purpose not specified in this agreement.

3. Records provided by Fiscal Service will not be duplicated or disseminated within or outside CMS, except as required by Federal law, without the written permission of Fiscal Service.
4. Access to match results from this matching program must be restricted to users (employees or contractors) who need to access Treasury's Working System for their official duties. CMS must evaluate which users require such access before the information is disclosed. If a user needs to know some information that does not mean the employee needs to know all information provided to CMS. Access must be strictly limited to those with a need to know in order to perform a legitimate business function related to the purpose of this matching agreement.

X. ACCURACY ASSESSMENTS

Through this matching agreement, CMS acknowledges that the information Fiscal Service provides is an accurate copy of the original source agency data. Any identified discrepancies in the data by either party to this matching agreement shall be referred immediately to the agency for which the record pertains for correction and a prompt refresh in Treasury's Working System.

XI. ACCESS BY THE OFFICE OF THE INSPECTORS GENERAL AND GOVERNMENT ACCOUNTABILITY OFFICE

The Government Accountability Office and the parties' Inspectors General Offices may have access to all records subject to this agreement as necessary in order to verify compliance with this agreement.

XII. LIMITATIONS

The terms of this agreement are not intended to alter, amend, or rescind any current agreement or provision of Federal law now in effect. Any provision of this agreement which conflicts with Federal law is null and void.

XIII. CONTINGENCY CLAUSE

Matches under this agreement may be immediately discontinued, if at any time, Fiscal Service or CMS determines that either party has failed to perform any of the terms of this agreement.

XIV. REPORT TO CONGRESS

When this agreement is approved by the Chairpersons of the CMS and Fiscal Service DIBs, CMS will submit a report of the proposed matching program to Congress and the OMB for review.

XV. REIMBURSEMENT FUNDING

All work to be performed by Fiscal Service to execute this matching program via Treasury's Working System in accordance with this agreement will be performed on a non-reimbursable basis, in accordance with legal agreements between CMS and Fiscal Service.

XVI. APPROVAL AND DURATION OF AGREEMENT

A. Pursuant to IPERIA, this matching agreement, as executed by representatives of both agencies, and approved by the respective agency DIBs, shall be valid for a period of less than 3 years from the effective date of the agreement.

B. When this agreement is approved and signed by the Chairpersons of the respective DIBs, CMS, as the recipient agency, will submit the agreement and the proposed public notice of the match as attachments in duplicate via a transmittal letter to OMB and Congress for review. The time period for review begins as of the date of the transmittal letter. A copy of the proposed Federal Register notice is in Attachment 4.

C. CMS will forward the public notice of the proposed matching program for publication in the Federal Register as required by subsection (e) (12) of the Privacy Act, at the same time the transmittal letter is forwarded to OMB and Congress. The matching notice will clearly identify the record systems and category of records being used and state that the program is subject to review by OMB and Congress. A copy of the published notice shall be provided to Fiscal Service.

D. This agreement may be extended for not more than 3 years subject to the requirements of the Privacy Act and IPERIA, including certification by the Parties to their respective DIBs that:

1. The matching program will be conducted without change, and
2. The matching program has been conducted in compliance with the original agreement.

E. This agreement may be modified at any time by a written modification to this agreement that satisfies both parties and is approved by the DIBs of the Parties.

F. This agreement may be terminated at any time with the consent of the Parties. If either CMS or Fiscal Service does not want to continue this matching program, it should notify the other party of its intention to discontinue the matching program at least 90 days before the end of the then current period of the agreement. Either party may unilaterally terminate this agreement upon written notice to the other party requesting termination, in which case the termination shall be effective 90 days after the date of the notice, or at a later date specified in the notice, provided the expiration date does not exceed the original, or the extended completion date, of the match.

XVII. PERSONS TO CONTACT

A. The contacts on behalf of Treasury are:

1. David Ambrose
   Chief Privacy Officer
   Bureau of the Fiscal Service
   Department of the Treasury
   Office: (202) 874–6488
   E-Mail: David.Ambrose@fiscal.treasury.gov

2. Kevin R. Jones

   Executive Director
   Do Not Pay Business Center
   Department of the Treasury
   Office: (202) 504-3516
   E-Mail: Kevin.Jones@fiscal.treasury.gov

3. Marcela Souaya

   Senior Privacy Analyst
   Do Not Pay Business Center
   Department of the Treasury
   Office: (202) 504-3525
   E-Mail: Marcela.Souaya@fiscal.treasury.gov

B. The contacts on behalf of CMS are:

1. Walter Stone

   CMS Privacy Officer
   Division of Privacy Policy
   Privacy Policy & Compliance Group
   Office of E-Health Standards & Services
   7500 Security Boulevard, Mail Stop S2-24-25
   Baltimore, MD 21244-1805
   Office: 410-786-5357
   E-mail: Walter.Stone@cms.hhs.gov

2. John Sofokles

   Government Technical Lead
   Center for Program Integrity (CPI)
   Data Analytics and Control Group (DACG)
   Systems Management Division (SMD)
   7500 Security Boulevard, Mail Stop AR-08-55
   Baltimore, MD 21244-1805
   Office: 410-786-6373
   E-mail: john.sofokles@cms.hhs.gov

XVIII. SIGNATURES

In witness whereof, the parties hereby execute this agreement.

U. S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

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

_____ Date: _____

Todd A. Lawson
Acting Director
Office of E-Health Standards & Services, and
Acting Senior Agency Official for Privacy

XIX. SIGNATURES

In witness whereof, the parties hereby execute this agreement.

BUREAU OF THE FISCAL SERVICE

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

_____ Date: _____

Kevin R. Jones
Do Not Pay Executive Director
Bureau of the Fiscal Service
Department of the Treasury

XX. SIGNATURES

In witness whereof, the parties hereby execute this agreement.

BUREAU OF THE FISCAL SERVICE
Data Integrity Board

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

_____ Date: _____

David Ambrose
Chief Privacy Officer
Bureau of the Fiscal Service
Department of the Treasury

XXI. SIGNATURES

In witness whereof, the parties hereby execute this agreement.

DEPARTMENT OF THE TREASURY
Data Integrity Board

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

_____ Date: _____

Helen Goff Foster
Chairperson
Data Integrity Board
Department of the Treasury

XXII. SIGNATURES

A. The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this agreement.

U. S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Data Integrity Board

The respective Data Integrity Board having reviewed this agreement and finding that it complies with applicable statutory and regulatory guidelines signify their respective approval thereof by the signature of the officials appearing below.

_____ Date: _____

E.J. Holland, Jr.
Chairperson
Data Integrity Board
Department of Health and Human Services

Attachments:

Attachment 1: Treasury/Bureau of the Fiscal Service .023 – Do Not Pay Payment Verification Records
Attachment 2: ‘‘Provider Enrollment, Chain, and Ownership System (PECOS),’’ System No. 09–70–0532
Attachment 3: Treasury’s Working System Data Elements
Attachment 4: Proposed *Federal Register* Notice

ATTACHMENT 1

DEPARTMENT OF THE TREASURY
Bureau of the Fiscal Service
Privacy Act of 1974, as Amended;
System of Records

AGENCY: Bureau of the Fiscal Service, Department of the Treasury.

ACTION: Notice of new Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, as amended, 5 U.S.C. 552a, the Department of the Treasury proposes to establish a new system of records entitled, ‘‘Department of the Treasury/Bureau of the Fiscal Service .023—Do Not Pay Payment Verification Records.’’ This system of records allows the Department of the Treasury/Bureau of the Fiscal Service to collect, maintain, analyze, and disclose records that will assist Federal agencies in identifying, preventing, and recovering payment error, waste, fraud and abuse within Federal spending as required by the Improper Payment Elimination and Recovery Improvement Act of 2012 (IPERIA), 31 U.S.C. 3321 note, Public Law 112–248. Information regarding the operation of this system of records and additional privacy protections (e.g., additional disclosure restrictions, active computer matching agreements, additional safeguards, etc.) can be found at *www.donotpay.treas.gov*.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), the public is given a 30-day period in which to comment. Therefore, comments must be received no later than January 8, 2014. If no comments are received, the system will become effective on January 21, 2014.

ADDRESSES: Comments may be sent by mail or electronic mail (email). Mail address: Disclosure Officer, Bureau of the Fiscal Service, 401 14th Street SW., Washington, DC 20227. Email Address: David.Ambrose@fiscal.treasury.gov. Comments received will be available for inspection by appointment at the address listed above between the hours of 9 a.m. and 4 p.m. Monday through Friday.

FOR FURTHER INFORMATION CONTACT:
For general questions please contact: Kevin R. Jones, Executive Director, Do Not Pay Business Center, 401 14th Street SW., Washington, DC 20227, Phone: (202) 504–3516, Bureau of the Fiscal Service, Email: Kevin.Jones@fiscal.treasury.gov.

For privacy issues please contact:
David Ambrose, Chief Privacy Officer, Bureau of the Fiscal Service,
3700 East-West Highway, Room 803–A, Hyattsville, MD 20782, Phone: (202) 874–6488, Email: David.Ambrose@fiscal.treasury.gov.

SUPPLEMENTARY INFORMATION:
I. Background

Federal agencies make more than $2 trillion in payments for contracts, grants, loans, benefits, and other congressionally-authorized purposes to individuals and a variety of other entities each year. Most of these payments are proper. However, improper payments occur when (a) funds go to the wrong recipient; (b) the recipient receives the incorrect amount of funds; (c) documentation is not available to support a payment; or (d) the recipient receives the funds in an improper or fraudulent manner. In accordance with the Improper Payment Elimination and Recovery Improvement Act of 2012 (IPERIA), the Office of Management and Budget (OMB) designated the Department of the Treasury to host the Do Not Pay Working System, also known as the Treasury Working System, which will help Federal agencies verify that their payments are proper before a payment is made. The Do Not Pay Working System will provide authorized Federal agencies with centralized access to various data sources, as well as access to analytical services designed to detect fraud and systemic improper payments. Treasury's Do Not Pay Working System also can help agencies identify why improper payments are made, so that agencies can take action to avoid future improper payments. By strengthening and enhancing financial management controls, Federal agencies can better detect and prevent improper payments and bolster taxpayer confidence in the Federal Government's management of taxpayer dollars. Under current practices, Federal agencies use information from multiple data sources to verify eligibility of a benefit recipient, loan applicant, contractor, grantee, or other recipient of Federal payments at various times during the payment cycle, most significantly pre-award and prepayment. Examples of data sources include the Department of Health and Human Services' List of Excluded Individuals/Entities, which contains information about individuals excluded from participation in Federal healthcare programs, such as Medicare, and the General Services Administration's System for Award Management (formerly the Excluded Parties List System), which contains information about contractors who are barred from doing business with the Federal Government. Typically, agencies do not solely rely on information contained in a single data source to make eligibility determinations, but use the data to confirm or supplement information received from the payment recipient and through other means. By centralizing access to multiple relevant data sources, Treasury is able to provide agencies with information to help them make better and timelier eligibility decisions. The Do Not Pay Working System provides authorized agencies with information about intended and actual payees of Federal funds in two ways. First, the Do Not Pay Working System enables authorized Federal agencies to access information from multiple databases through a central web portal maintained by Treasury. Second, Treasury compares information about payees from payment files submitted by Federal paying agencies to information contained in multiple data sources. For both methods, the paying agency reviews any data provided by the Do Not Pay Working System to determine whether the data are correct and how the data impacts payment eligibility in accordance with program-specific eligibility rules and procedures. In addition, Treasury provides data analysis that helps agencies detect fraud and improve internal controls to systemically prevent, identify, and recover improper payments. Only authorized Federal agency personnel with appropriate security credentials may access the data available through the Do Not Pay Working System. Some of the data made available through the Do Not Pay Working System is subject to the Privacy Act of 1974. OMB Memorandum M–13–20 (Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative), which implemented section 5 of IPERIA, made it clear that Treasury is authorized to establish a system of records to carry out activities described in the statute. As required by 5 U.S.C. 552a(r) of the Privacy Act, the report of a new system of records has been provided to the

House of Representatives Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and OMB. The proposed new system of records, entitled ‘‘Bureau of the Fiscal Service .023 Do Not Pay Payment Verification Records’’ is published in its entirety below.

II. Public Disclosure

Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment including your personal identifying information may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Dated: December 4, 2013.
Helen Goff Foster,
Deputy Assistant Secretary for Privacy, Transparency, and Records.

TREASURY/Fiscal Service .023

SYSTEM NAME:
Do Not Pay Payment Verification Records—Department of the Treasury/Bureau of the Fiscal Service.

SYSTEM LOCATION:
Records are maintained at the Bureau of the Fiscal Service, United States Department of the Treasury, Washington, DC 20227. Records are also located throughout the United States at Fiscal Service operations centers, Federal Records Centers, Federal Reserve Banks acting as Treasury’s fiscal agents, and financial institutions acting as Treasury’s financial agents. The specific address for each of the aforementioned locations may be obtained upon request.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
(a) Individuals who have applied for or are receiving payments (including contract, grant, benefit or loan payments) disbursed by any Federal agency, its agents or contractors; (b) Individuals declared ineligible to participate in Federal procurement programs or to receive certain Federal loans, assistance, and/or benefits as a result of an exclusion or disqualification action; (c) Individuals declared ineligible to participate in Federal health care programs or to receive Federal assistance and/or benefits as a result of an exclusion action; (d) Individuals who are barred from entering the United States; (e) Individuals in bankruptcy proceedings or individuals who have declared bankruptcy; (f) Individuals who are, or have been, incarcerated and/or imprisoned; (g) Individuals who are in default or delinquent status on loans, judgment debt, or rural development and farm services programs provided through Federal agencies responsible for administering Federally-funded programs; (h) Individuals who owe non-tax debts to the United States; (i) Individuals who owe debts to states, where the state has submitted the debt to the Bureau of the Fiscal Service for offset; and (j) Individuals conducting, or attempting to conduct, transactions at or through a financial institution where the financial institution has identified, knows, suspects, or has reason to suspect that: (1) The transaction involves funds originating from illegal activities; (2) the purpose of the transaction is to hide or disguise funds or assets, or attempt to hide or disguise funds or assets, originating from illegal activities as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under

Federal law; or (3) the transaction is illegal in nature or is not the type of transaction in which the particular individual would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

CATEGORIES OF RECORDS IN THE SYSTEM:
The records in this system contain information that will assist Federal agencies to identify and prevent payment error, waste, fraud, and abuse within Federal spending. The records contain information about intended or actual payees or recipients of Federal payments, including information about financial assets, including income, wages, and bank accounts into which payments are made, and other information to assist Federal agencies in making eligibility determinations regarding applicants for and recipients of payments from the Federal Government. The records may contain the following information: (a) Name(s), including aliases and surnames; (b) State and Federal Taxpayer Identification Number (TIN), Social Security Number (SSN), Employer Identification Number (EIN), Individual Taxpayer Identification Number (ITIN), Taxpayer Identification Number for Pending U.S. Adoptions (ATIN), and Preparer Taxpayer Identification Number (PTIN)); (c) Date of birth; (d) Home and work address; (e) Driver's license information and other information about licenses issued to an individual by a governmental entity; (f) Home, work, and mobile telephone numbers; (g) Personal and Work email addresses; (h) Income; (i) Employer information; (j) Assets and bank account information, including account number and financial institution routing and transit number; (k) Other types of accounts to which payments are made, including account numbers and identifiers (e.g., financial institution routing number, account number, credit card number, and information related to pre-paid debit cards); (l) Tracking numbers used to locate payment information; (m) Loan information, such as borrower identification (ID) number and ID type, case number, agency code, and type code; (n) Incarceration information, such as inmate status code, date of conviction, date of confinement, and release date; (o) Information about legal judgments; (p) Data Universal Numbering System (DUNS) numbers; (q) Information about non-tax debts owed to the United States; and (r) Information about debts owed to state agencies.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
Improper Payments Elimination and Recovery Improvement Act of 2012, 31 U.S.C. 3321 note, Public Law 112–248; The Improper Payments Elimination and Recovery Act of 2010, Public Law 111–204; E.O. 13520 (Reducing Improper Payments and Eliminating Waste in Federal Programs), 74 FR 62201; OMB Memorandum M–13–20 (Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative); Presidential Memorandum on Enhancing Payment Accuracy through a ''Do Not Pay List'' (June 18, 2010).

PURPOSE(S):
This system of records will assist Federal agencies in verifying that individuals are eligible to receive Federal payments by allowing the Department of the Treasury/Bureau of the Fiscal Service to collect, maintain, analyze, and disclose records that will assist Federal agencies in identifying, preventing, and recovering payment error, waste, fraud, and abuse within Federal spending, as required by IPERIA.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

This system contains records that are collected by the Bureau of the Fiscal Service and other Federal agencies. The routine uses for this system of records are listed below. Federal law may further limit how records may be used, and the Bureau of the Fiscal Service may agree to additional limits on disclosure for some data through a written agreement with the entity that supplied the information. As such, the routine uses detailed below may not apply to every data set in the system. To identify which routine uses apply to specific data sets, visit *www.donotpay.treas.gov*. (a) Disclosure to (1) a Federal agency, its employees, agents (including contractors of its agents) or contractors; or (2) a fiscal or financial agent designated by the Bureau of the Fiscal Service, its predecessors, or other Department of the Treasury bureau or office, including employees, agents or contractors of such agent; or (3) a Bureau of the Fiscal Service contractor, for the purpose of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds; (b) Disclosure to a congressional office in response to an inquiry from the individual to whom the record or information pertains; (c) Disclosure to (1) a Federal agency, its employees, agents (including contractors of its agents) or contractors; or (2) a fiscal or financial agent designated by the Bureau of the Fiscal Service, its predecessors, or other Department of the Treasury bureau or office, including employees, agents or contractors of such agent; or (3) a Bureau of the Fiscal Service contractor, to initiate an investigation, or during the course of an investigation, and to the extent necessary, obtain information supporting an investigation pertinent to the elimination of systemic fraud, waste, and abuse within Federal programs; (d) Disclosure to (1) a Federal agency, its employees, agents (including contractors of its agents) or contractors; or (2) a fiscal or financial agent designated by the Bureau of the Fiscal Service, its predecessors, or other Department of the Treasury bureau or office, including employees, agents or contractors of such agent; or (3) a Bureau of the Fiscal Service contractor for the purpose of validating eligibility for an award through a Federal program; (e) Disclosure to (1) a Federal agency, its employees, agents (including contractors of its agents) or contractors; or (2) a fiscal or financial agent designated by the Bureau of the Fiscal Service, its predecessors, or other Department of the Treasury bureau or office, including employees, agents or contractors of such agent; or (3) a Bureau of the Fiscal Service contractor to check or improve the quality and accuracy of system records; (f) Disclosure to financial institutions and their servicers in order (1) to verify the proper routing and delivery of any Federal payment; (2) to verify the identity of any recipient or intended recipient of a Federal payment; or (3) to investigate or pursue recovery of any improper payment; (g) Disclosure to appropriate Federal agencies responsible for investigating or prosecuting violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of a possible violation of civil or criminal law or regulation; (h) Disclosure to a Federal agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, which has requested information relevant or necessary to the requesting agency's hiring or retention of an individual or issuance of a security clearance, license, contract, grant, or other benefit; (i) Disclosure to a court, magistrate, mediator, or administrative tribunal in the course of presenting evidence to counsel, experts, or witnesses in the course of civil discovery, litigation, or settlement negotiations, in response to a subpoena, or in connection with criminal law proceedings; (j) Disclosure to appropriate agencies, entities, and persons when (1) the Department of the Treasury suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or

another agency or entity) that relies upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:
Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The electronic records are stored on magnetic disc, tape, and electronic media.

RETRIEVABILITY:
Records may be retrieved by identifiers, including, but not limited to, exact name, partial name, SSN, TIN, EIN, DUNS numbers, or a combination of these elements.

SAFEGUARDS:
System records are safeguarded in accordance with the requirements of the Privacy Act. Access to the Treasury's Working System is available only by authorized individuals on a need-to know basis. External access logs to Treasury's Working System are reviewed to ensure compliance with rules of behavior agreed to by credentialed users. Internal access log control measures are reviewed to ensure compliance with security guidelines governing access to Privacy Act data. Audit logs allow system managers to monitor external and internal user actions and address any misuse or violation of access privileges. Access to computerized records is limited through the use of internal mechanisms available to only those whose official duties require access. Facilities where records are physically located are secured by various means, such as security guards, locked doors with key entry, and equipment requiring a physical token to gain access. The Bureau of the Fiscal Service may agree to additional safeguards for some data through a written agreement with the entity supplying the data. Information on additional safeguards can be found at *www.donotpay.treas.gov*.

RETENTION AND DISPOSAL:
Records in this system created or collected by the Bureau of the Fiscal Service are governed by a NARA records schedule, and are generally retained for a maximum of seven years after the end of the fiscal year in which the record was created. Pursuant to Section 7(b) of OMB Memorandum 13–20, the Bureau of the Fiscal Service will retain and dispose of records supplied by other Federal agencies in accordance with our written agreements with those agencies. Information on additional retention and disposal requirements can be found at *www.donotpay.treas.gov*.

SYSTEM MANAGER(S) AND ADDRESS:
Executive Director, Do Not Pay Business Center, Bureau of the Fiscal Service, 401 14th Street SW., Washington, DC 20227.

NOTIFICATION PROCEDURE:
Inquiries under the Privacy Act of 1974, as amended, should be addressed to the Disclosure Officer, Bureau of the Fiscal Service, 401 14th Street SW.,

Washington, DC 20227. Individuals should describe the information they seek as specifically as possible. If an individual requests that information in a record be corrected, the system manager will advise the requestor where to send the request. Ordinarily, data errors must be corrected by the entity that supplied the data to Treasury's Working System. Treasury will follow procedures for the accuracy and correction of information in the system that is described in OMB Memorandum M–13–20, available at *http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-20.pdf*. Information concerning Privacy Act requests are published at 31 CFR Part 1, Subpart C, and Appendix G. The Bureau of the Fiscal Service may agree to additional notification procedures for some data through a written agreement with the supplying entity. Information on additional notification procedures can be found at *www.donotpay.treas.gov*.

RECORD ACCESS PROCEDURES:
See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:
See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:
Information in this system is provided by the individual (or an authorized representative) to whom the record pertains, Federal agencies that authorize payments or issue payments with Federal funds, Treasury fiscal and financial agents who work with data in this system, and commercial database vendors. The system may contain information about an individual from more than one source, and this information may vary, depending on the source that provided it.

EXEMPTIONS CLAIMED FOR THE SYSTEM:
None.

ATTACHMENT 2

SYSTEM NO. 09-70-0532

SYSTEM NAME:
"Provider Enrollment, Chain, and Ownership System (PECOS), HHS/CMS/OFM"

SECURITY CLASSIFICATION:
Level Three Privacy Act Sensitive Data

SYSTEM LOCATION:

The Centers for Medicare & Medicaid Services (CMS) Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244-1850 and South Building, Baltimore, Maryland 21244-1850.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

PECOS will collect information provided by the applicant related to identity, qualifications, practice locations, ownership, billing arrangements, reassignment of benefits, surety and bond data, clearinghouses submitting electronic claims, and related organizations. PECOS will also maintain information on business owners, chain home offices and provider/chain associations, managing/directing employees, partners, authorized and delegated representatives, supervising physicians of the supplier, staffing companies, ambulance crew members, and/or interpreting physicians and related technicians.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system of records will contain the names, social security numbers (SSN), and employer identification numbers (EIN) for each disclosing entity, owners, as well as managing/directing employees, with 5 percent or more ownership or control interest. Managing/directing employees include general manager, business managers, administrators, directors, and other individuals who exercise operational or managerial control over the provider/supplier. The system will also contain the Unique Provider Identification Number, demographic data, professional data, past and present business history as well as information regarding any exclusions, sanctions, and felonious behavior.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Authority for maintenance of the system is given under provisions of sections 1102(a) (Title 42 U.S.C. 1302(a)), 1128 (42 U.S.C. 1320a-70), 1814(a) (42 U.S.C. 1395f(a)(1), 1815(a) (42 U.S.C. 1395g(a)), 1833(e) (42 U.S.C. 1395(e), 1871 (42 U.S.C. 1395hh), and 1886(d)(5)(F), (42 U.S.C. 1395ww(d)(5)(F) of the Social Security Act; 1842(r) (42 U.S.C. section 9202(g)); section 1124(a)(1) (42 U.S.C. 1320a-3(a)(1), and 1124A (42 U.S.C. 1320a-3a), section 4313, as amended, of the BBA of 1997; and section 31001(I) (31 U.S.C. 7701) of the DCIA (P.L. 104-134), as amended.

PURPOSE(S) OF THE SYSTEM:

The primary purpose of the SOR is to: (1) collect information for an applying provider/supplier and record the associations between the applicant and those who have an ownership or control interest in the entity; (2) permit informed enrollment decisions to be made based on past and present business history, any reported exclusions, sanctions and felonious behavior at their location or in multiple contractor jurisdictions; and, (3) ensure that correct payments are made under the Medicare program. Information retrieved from this SOR will also be disclosed to: (1) support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor or consultant; (2) assist another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent; (3) assist an individual or organization for research; (5) support litigation involving the Agency; and (5) combat fraud and abuse in certain health benefits programs.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OR USERS AND THE PURPOSES OF SUCH USES:

The Privacy Act allows us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such compatible use of data is known as a "routine use." The proposed routine uses in this system meet the compatibility requirement of the Privacy Act. We are proposing to establish the following routine use disclosures of information maintained in the system:

To support agency contractors, consultants, or grantees, who have been engaged by the agency to assist in the performance of a service related to this collection and who need to have access to the records in order to perform the activity.

To assist another Federal or state agency, agency of a state government, an agency established by state law, or its fiscal agent to:

contribute to the accuracy of CMS's proper payment of Medicare benefits, enable such agency to administer a Federal health benefits program, or as necessary to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with federal funds evaluate and monitor the quality of home health care and contribute to the accuracy of health insurance operations.

To assist an individual or organization for research, evaluation or epidemiological projects related to the prevention of disease or disability, or the restoration or maintenance of health, and for payment related projects.

To support the Department of Justice (DOJ), court or adjudicatory body when:

the agency or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee, or

the United States Government is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and that the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

To assist a CMS contractor (including, but not necessarily limited to fiscal intermediaries and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, or abuse in such program.

To assist another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any State or local governmental agency), that administers, or that has the authority to investigate potential fraud or abuse in, a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, or abuse in such programs.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

All records are stored on paper and magnetic disk.

RETRIEVABILITY:

Magnetic media records are retrieved by the name of the employees or other authorized individual and/or card key number. Paper records are retrieved alphabetically by name.

SAFEGUARDS:

CMS has safeguards in place for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations may apply but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-Government Act of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A-130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, HHS, and CMS policies and standards include but are not limited to: all pertinent National Institute of Standards and Technology publications; the HHS Information Systems Program Handbook and the CMS Information Security Handbook.

RETENTION AND DISPOSAL:

CMS will retain identifiable data for a total period of 15 years from the date the information was collected.

SYSTEM MANAGERS AND ADDRESS:

Director, Division of Provider/Supplier Enrollment, Office of Financial Management, CMS, 7500 Security Boulevard, Baltimore, Maryland 21244-1850.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the system manager who will require the system name, SSN, EIN, and for verification purposes, the subject individual's name (woman's maiden name, if applicable).

RECORD ACCESS PROCEDURE:

For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5(a)(2).)

CONTESTING RECORD PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the record and specify the information to be contested. State the corrective action

sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7.)

RECORD SOURCE CATEGORIES:

Information contained in this system is received from the Form(s) HCFA 855A, "Application for Health Care Providers that will Bill Medicare Fiscal Intermediaries, HCFA 855B, "Application for Health Care Providers that will Bill Medicare Carriers," HCFA 855I, "Application for Individual Health Care Practitioners," HCFA 855R, "Application for Reassignment of Medicare Benefits," and HCFA 855S, "Durable Medial Equipment, Prosthetics, Orthotics, and Suppliers Application."

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

ATTACHMENT 3

Treasury's Working System data elements include, but are not limited to:

SAM Exclusions (formerly Excluded Parties List System/EPLS)

i. SAM NUMBER
ii. DUNS
iii. NPI
iv. CAGE
v. NAME
vi. PREFIX
vii. FIRST
viii. MIDDLE
ix. LAST
x. SUFFIX
xi. SSN
xii. TIN
xiii. EXCLUSION PROGRAM
xiv. CLASSIFICATION
xv. ADDRESS
xvi. CITY
xvii. ZIP
xviii. STATE
xix. COUNTRY
xx. ACTION DATE
xxi. TERM DATE
xxii. EXCLUSION TYPE
xxiii. AGENCY SAM NUMBER
xxiv. AGENCY NAME
xxv. DESCRIPTION
xxvi. SAM CREATE DATE
xxvii. CLASSIFICATION

ATTACHMENT 4

Proposed *Federal Register* Notice
Computer Matching Program

DEPARTMENT OF HEALTH AND HUMAN SERVICES

CENTERS FOR MEDICARE & MEDICAID SERVICES

Privacy Act of 1974

CMS Computer Match No. 2014-04

HHS Computer Match No. 1402

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, The Improper Payments Elimination and Recovery Improvement Act of 2012 ,Pub. L. 112-248, 126 Stat. 2390; and OMB Memorandum M-13-20 (Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative); this notice announces the establishment of a CMP that HHS plans to conduct with the Bureau of the Fiscal Service (Fiscal Service). We have provided background information about the proposed matching program in the "Supplementary Information" section below. Although the Privacy Act requires only that CMS provide an opportunity for interested persons to comment on the proposed matching program, CMS invites comments on all portions of this notice. See "Effective Dates" section below for comment period.

EFFECTIVE DATES: Public comments are due 30 days after publication. The 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.

ADDRESS: The public should send comments to: CMS Privacy Officer, Division of Privacy Policy, Privacy Policy and Compliance Group, Office of E-Health Standards & Services, Office of Enterprise Management, CMS, Room S2-24-25, 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: John Sofokles, Government Technical Lead, Systems Management Division (SMD), Data Analytics and Control Group (DACG), Center for Program Integrity (CPI), CMS, Mail Stop AR-18-50, 7500 Security Boulevard, Baltimore, MD 21244-1805, Office Phone: 410-786-6373, E-mail: john.sofokles@cms.hhs.gov

SUPPLEMENTARY INFORMATION:

I. DESCRIPTION OF THE MATCHING PROGRAM

A. General

The Computer Matching and Privacy Protection Act of 1988 (Public Law (Pub. L.) 101-503), 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 (SOR) are matched with other Federal, state, or local government records. It requires Federal agencies involved in computer matching programs to:

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

B. CMS Computer Matches Subject to the Privacy Act

CMS has taken action to ensure that all CMPs that this Agency participates in comply with the requirements of the Privacy Act of 1974, as amended, The Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. 112-248, 126 Stat. 2390; and OMB Memorandum M-13-20 (Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative).

Date: _____

_____

Celeste Dade-Vinson
Health Insurance Specialist
Centers for Medicare & Medicaid Services

CMS Computer Match No. 2014-04

HHS Computer Match No. 1402

NAME: "Computer Matching Agreement between the Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services and the Bureau of the Fiscal Service (Fiscal Service) for access to the Treasury/Bureau of the Fiscal Service .023—Do Not Pay Payment Verification Records," by CMS via matching services provided through Treasury's Working System and authorized by section 5 of IPERIA"

SECURITY CLASSIFICATION:

Unclassified

PARTICIPATING AGENCIES:

Department of Health and Human Services, Centers for Medicare & Medicaid Services and the Department of Treasury/Bureau of the Fiscal Service (Fiscal Service).

AUTHORITY FOR CONDUCTING MATCHING PROGRAM:

This Computer Matching Program (CMP) is executed to comply with the provisions of the Privacy Act of 1974 (5 U.S.C. 552a), as amended, The Improper Payments Elimination and Recovery Improvement Act of 2012 ,Pub. L. 112-248, 126 Stat. 2390.; OMB Memorandum M-13-20 (Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative); the Office of Management and Budget (OMB) Circular A-130 entitled, Management of Federal Information Resources, at 61 FR 6428-6435 (February 20, 1996), and OMB guidelines pertaining to computer matching at 54 FR 25818 (June 19, 1989) and 56 FR 18599 (April 23, 1991); and the computer matching portions of Appendix I to OMB Circular No. A-130 as amended at 61 Fed. Reg. 6428, February 20, 1996;

PURPOSE (S) OF THE MATCHING PROGRAM:

The purpose of this matching program is to reduce improper payments by authorizing Fiscal Service to provide HHS, through the U.S. Department of the Treasury's Working System as defined by OMB Memorandum M-13-20 (Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative), identifying information from Fiscal Service's system of records Treasury/Fiscal Service .023 about individuals and entities excluded from receiving federal payments, contract awards, and other benefits. The information resulting from this matching program will be provided to CMS in determining whether an individual or entity is eligible to receive federal payments, contract awards or other benefits. Using a computer matching program for this purpose eliminates the need for each payment, procurement and benefit program to execute several Memoranda of Agreement with multiple federal agencies, provides access to up-to-date information, and avoids the need to manually compare files.

DESCRIPTION OF RECORDS TO BE USED IN THE MATCHING PROGRAM

System of Records Maintained by Fiscal Service

Fiscal Service will provide HHS with information comprised of match results originating from the matching activities between HHS system of records data and Fiscal Service's Treasury/Fiscal Service .023, as published at 78 Federal Register (Fed. Reg.), 73923, December 9, 2013. Fiscal Service data will be used in matching activities and match results released to HHS via Treasury's Working System.

Systems of Records Maintained by CMS

The matching program will be conducted with data maintained by CMS in the ''Provider Enrollment, Chain, and Ownership System (PECOS),'' System No. 09–70–0532, established at

66 Fed. Reg., 51961 (October 11, 2001). PECOS routine use number 2 will allow PECOS data to be disclosed to Fiscal Service to assist Fiscal Service in contributing to the accuracy of CMS Medicare benefit payments. PECOS routine use number 1 will allow match results data that PECOS obtains from Treasury's Working System to be disclosed to CMS contractors, consultants, and grantees assisting CMS with PECOS purposes.

INCLUSIVE DATES OF THE MATCH:

The CMP shall 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 36 months from the effective date and may be extended for an additional 12 months thereafter, if certain conditions are met.