US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/01/2016

OPDIV:

CMS

Name:

Unified Case Management System

PIA Unique Identifier:

P-3626618-952714

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

Unified Case Management (UCM) system and associated operational services provide a central repository to support the workload of direct contractors for Centers for Medicare and Medicaid Services (CMS) Program Integrity Contractors (PICs) including Zone Program Integrity Contractors (ZPICs), Program Safeguard Contractors (PSCs), Medicaid Integrity Contractors (MICs), Medicare Drug Integrity Contractors (MEDICs) and future Unified Program Integrity Contractors (UPICs) -- all of which are direct contractors-- across the Medicare and Medicaid programs in their efforts to mitigate fraud, waste and abuse within the programs. This workload includes providing the capability to track leads, audits and investigations; capture and manage workflow activities; report workload metrics; report status of administrative actions and referrals to law enforcement; and record outcomes or disposition of program integrity audit and investigative actions across Medicare and Medicaid programs.

Describe the type of information the system will collect, maintain (store), or share.

The system contain information including the name, work address, work phone number, social security number, Unique Provider Identification Number (UPIN), National Provider Identifier (NPI), medical notes, foreign activities, device identifiers and financial account information of individuals alleged to have violated provision of the Social Security Act or persons alleged to have abused Medicare and/or Medicaid programs. The system will collect PII from CMS employees and direct contractor input (user IDs and passwords). The management and maintenance of the user information in order to create user accounts for UCM is handled within CMS' Enterprise User Administration (EUA) and Enterprise ID Management (EIDM).

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The primary purpose of this system is to collect and maintain information to: (1) Identify a violation or violations of a provision of the Social Security Act or a related penal or civil provision of the United States Code related to Medicare, Medicaid, Health Maintenance Organization (HMO)/Managed Care, and Children's Health Insurance Program have been committed; (2) determine if CMS has made a proper payment as prescribed under applicable sections of the Act; (3) determine whether these programs have been abused; 4) coordinate investigations related to Medicare, Medicaid, HMO/Managed Care and Children's Health Insurance Program (CHIP); (5) prevent duplications of investigatory efforts; and (6) provide case file material to the HHS Office of Inspector General and other federal law enforcement agencies when a case is referred for fraud investigation.   UCM will also share PII data with other CMS legacy systems.

The user ID and password will be collected for internal system users. The management and maintenance of the user information in order to create user accounts for UCM is handled within CMS' Enterprise User Administration (EUA) and Enterprise ID Management (EIDM).

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number

Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Notes

Financial Accounts Info

Device Identifiers

Foreign Activities

Other: Unique Provider Identification Number (UPIN), National Provider Identifier (NPI), user ID and

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The PII is used for CMS fraud, waste and abuse investigations for supporting efforts to protect healthcare expenditures by supporting program integrity functions and combating fraud, waste and abuse in Medicare and Medicaid.

The PII for internal system users is used to gain system access in order to support system operations.

Describe the secondary uses for which the PII will be used.

The PII will be used and shared with other CMS legacy systems to validate Fraud, Waste and Abuse (FWA) outcomes, workload and return on investment.

Describe the function of the SSN.

The Social Security Number (SSN) is used as a data element identifier to assist in identifying an individual within the system in the analysis of data for Fraud, Waste and Abuse.

Cite the legal authority to use the SSN.

This information collected is covered under the following SORNs. From Medicare Integrated Data Repository (MID) SORN 09-70-0571: Authority for the collection of data maintained in this system is given under section 226, 226A, 1811, 1818, 1818A, 1831, 1833(a)(1)(A), 1836, 1837, 1838, 1843, 1866, 1874a, 1875, 1876, 1881, and 1902(a)(6) of the Social Security Act (the Act). The following are the corresponding sections from Title 42 of the United States Code (U.S.C.): 426, 426–1, 1395c, 1395i–2, 1395i–2a, 1395j, 1395l(a)(1)(A), 1395o, 1395p, 1395q, 1395v, 1395cc, 1395kk–l, 1395ll, 1395mm, 1395rr, 1396a(a)(6), and section 101 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (Pub. L. 108–173), which established the Medicare Part D program.

and

From OnePI SORN 09-70-0568: Authority for maintenance of this system is given under section 1893 of the Social Security Act.

Sections 1816(a) and 1842(a) of the Social Security Act provide that public or private entities and agencies may participate in the administration of the Medicare program under agreements or contracts entered into with CMS. These Medicare Contractors are known as Fiscal Intermediaries (FIs) and Carriers. FIs have primarily processed bills and made payments for all facilities (hospitals, Skilled Nursing Facilities (SNFs), Ambulatory Surgical Centers (ASCs), etc.). Carriers have primarily processed claims and made payments for all Part B services billed by a physician or supplier.

As part of these contractual duties, FIs and Carriers were charged to perform program integrity activities. These activities include, among other things, reviewing claims to make coverage determinations and auditing provider cost reports. FIs and Carriers performed the entire range of claims processing functions, including entering data, establishing computer edits to identify potential duplicate claims, and mailing notices to beneficiaries and providers. In addition, FLs and Carrier has as part of their responsibilities to deter and detect potential fraud and/or abuse.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-191) was enacted on August 21, 1996. Section 202 of Public Law 104-191 added a new section, §1893, to the Act that established the Medicare Integrity Program (MIP). MIP was established, in part, to strengthen CMS' ability to deter potential fraud, waste and abuse in the Medicare program. It provides a separate and stable long-term funding mechanism for MIP activities. By expanding CMS' contracting authority, MIP allows CMS to more aggressively carry out program safeguard functions.

Section 6034 of the Deficit Reduction Act (DRA) of 2005 created the Medicaid Integrity Program and amended Title XIX of the Social Security Act (42 U.S.C. 1396 et seq.).

Section 4241 of the Small Business Jobs Act of 2010 (Public Law 111-240) mandates the use of predictive modeling and other analytic technologies to identify and prevent fraud, waste, and abuse in the Medicare FFS program.

Identify legal authorities governing information use and disclosure specific to the system and program.

Sections 1816(a) and 1842(a) of the Social Security Act provide that public or private entities and agencies may participate in the administration of the Medicare program under agreements or contracts entered into with CMS. These Medicare Contractors are known as Fiscal Intermediaries (FIs) and Carriers. FIs have primarily processed bills and made payments for all facilities (hospitals, Skilled Nursing Facilities (SNFs), Ambulatory Surgical Centers (ASCs), etc.). Carriers have primarily processed claims and made payments for all Part B services billed by a physician or supplier.

As part of these contractual duties, FIs and Carriers were charged to perform program integrity activities. These activities include, among other things, reviewing claims to make coverage determinations and auditing provider cost reports. FIs and Carriers performed the entire range of claims processing functions, including entering data, establishing computer edits to identify potential duplicate claims, and mailing notices to beneficiaries and providers. In addition, FIs and Carriers had as part of their responsibilities to deter and detect potential fraud and/or abuse.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-191) was enacted on August 21, 1996. Section 202 of Public Law 104-191 added a new section, §1893, to the Act that established the Medicare Integrity Program (MIP). MIP was established, in part, to strengthen CMS' ability to deter potential fraud, waste and abuse in the Medicare program. It provides a separate and stable long-term funding mechanism for MIP activities. By expanding CMS' contracting authority, MIP allows CMS to more aggressively carry out program safeguard functions.

Section 6034 of the Deficit Reduction Act (DRA) of 2005 created the Medicaid Integrity Program and amended Title XIX of the Social Security Act (42 U.S.C. 1396 et seq.).

Section 4241 of the Small Business Jobs Act of 2010 (Public Law 111-240) mandates the use of predictive modeling and other analytic technologies to identify and prevent fraud, waste, and abuse in the Medicare FFS program.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

Published: 09-70-0571 (Medicare Integrated Data)

Published: 09-70-0568 (One Program Integrity Data)

Published: UCM SORN (in progress with CMS Privacy office

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Other Federal Entities

Identify the OMB information collection approval number and expiration date

The UCM system does not directly interact with individuals to collect their information. The OMB information collection approval number and expiration date is not applicable.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

Data is shared with other CMS legacy systems. The information within the UCM system is used for investigative purposes.

Other Federal Agencies

Department of Justice (DOJ). The information within the UCM system is used for investigative purposes.

State or Local Agencies

State agencies overseeing Medicaid programs. The information within the UCM system is used for investigative purposes.

Describe any agreements in place that authorizes the information sharing or disclosure.

Memorandum of Understanding (MOU) between Centers for Medicare and Medicaid Services (CMS) & Health and Human Services Office of Inspector General (HHS OIG) and US Department of Justice Federal Bureau of Investigation (DOJ FBI).

Describe the procedures for accounting for disclosures.

The UCM system follows the CMS Acceptable Risk Safeguards (ARS) policy to track all disclosures to third parties. UCM requires that a CMS Data Use Agreement (DUA) is completed and approved by CMS before any disclosure of personally identifiable information is completed. This includes for other federal agencies and contracting partners. The DUA includes the requestor of the data, the record of the data that is being disclosed, and the authority that CMS has for disclosing the information. UCM also ensures that any disclosure to a CMS contracting partner occurs only when a business associate agreement is also in place for this organization to complete work on behalf of the government which would require access to personally identifiable information.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Information is posted to the UCM system by CMS approved contractors and investigators. Thus UCM does not directly collect personal information from individuals for the UCM system and does not have a process in place to notify individuals that their personal information will be collected.

UCM Systems administrators user ID and password is collected in order to authenticate their access to the system. Because this collection is required in order for them to conduct their required tasks no formal notice is provided them. The management and maintenance of the user information in order to create user accounts for UCM is handled within CMS' Enterprise User Administration (EUA) and Enterprise ID Management (EIDM).

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

The UCM system does not directly interact with individuals to collect their information. As the information posted in the UCM system is used for investigative purposes, there is no option to object to the information collection or to opt out.

The collection of this data is required under the Social Security Act for the participation of individuals in the Medicare and Medicaid services. Access to the data can only be obtained through the CMS internal network and requires identification and authorization through CMS EUA and EIDM processes.

UCM Systems administrator user ID and password is collected in order to authenticate their access to the system. Because this collection is required in order for them to conduct their required tasks no opt-out option is available.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

The UCM system has no process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system. The information in the database is posted by CMS approved contractors and investigators. The UCM system obtains the data from the CMS Shared Services system, CMS One Program Integrity System (OnePI), and the CMS Fraud Prevention System (FPS), therefore these systems as the system of record og the dtat, they will notify and obtain consent from individuals as major changes occur to the system and the associated data.

UCM Systems administrator user ID and password is collected in order to authenticate their access to the system. Because this collection is required in order for them to conduct their required tasks no formal notice is provided them when there is a major change to the system.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

CMS System of Records Notification Process. Access to the data can only be obtained through the CMS internal network and requires identification and authorization through CMS EUA and EIDM processes.

CMS System of Records Notification Process.

The information is aggregated to support statistical analysis and fraud, waste, and abuse investigations. Information about an individual is processed in support of these investigations.

NOTIFICATION PROCEDURE:
For purpose of access, the subject individual should write to the system manager who will require the system name, social security number (SSN) or UPIN, address, date of birth, and sex, and for verification purposes, the subject individual’s name (woman’s maiden name, if applicable). Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay.

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).

UCM System administrators user ID and password is collected in order to authenticate their access to the system. In the event the user's credentials are inaccurate the administrators and system users must contact the UCM service desk to initiate resolution of the issue. The concerns of the administrators and system users will be directly considered, investigated and resolved over the phone or through email exchange on a one-on-one bases by the UCM service desk personnel as required.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

CMS has safeguards in place for authorized users and monitors such users to ensure against 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. UCM users take required annual information security and privacy training to receive regular information on this.

The UCM system also follows the CMS Acceptable Risk Safeguards which details the requirements for data inspection, integrity, accuracy, and relevancy. If the system should undergo any major significant change to the system, an information security and privacy test is applied to ensure the protection of the PII data contained in the system. Technical controls used include user identification, passwords, security tokens, firewalls, virtual private networks, and intrusion detection systems. Physical controls used include guards, identification badges, key cards, cipher locks, and closed circuit televisions.

Any PII collected by UCM is in a read-only format. The data will not be able to be modified or destroyed. UCM is the aggregator of the information collected through investigations. It is not the function of the UCM application to validate data contained within the application, any more than it is the function of a word processing application to validate the veracity of the information contained in its documents. Therefore, UCM in not responsible for validating the data and information it aggregates from other sources. Data migration is tested based on source sample data to determine the proper importation of source data.

User IDs and passwords are maintained external to the UCM system in the CMS EUA and EIDM systems. UCM roles are administered through a UCM Lightweight Directory Access Protocol (LDAP server. Access to the UCM LDAP is dependent on valid EIDM credentials. If a user role changes permissions are updated in EIDM, and these changes are reselected in relevant LDAP provided access. The server is managed and backed up by Lockheed Martin as part of their infrastructure support services.

Because UCM is not responsible for the integrity, accuracy or relevancy of non-employee PII it contains there is no mechanism or process to review the data for these attributes.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

UCM users to complete Fraud, Waste and Abuse workload.

Administrators:

Management of the UCM system

Developers:

Enhancement of the UCM system.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Account management mechanisms are established for UCM through the CMS Enterprise Identity Management System (EIDM) to identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. UCM users are granted access based on the assigned duty and intended system use.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Logical access controls and procedures are established for UCM to ensure that only designated individuals can access the CMS information system. UCM team members with CMS EIDM and EUA User IDs re-take the CMS online Information Security and Privacy Training course and re-certify the “System Access” annually via CMS Extended User Authorization (EUA) Passport to continue accessing the approved CMS system(s). A process has been established for the UCM system when user access is no longer required, due to a change in role on the project or departure from the UCM project team, the UCM Project Manager and the CMS UCM Government Task Leader (GTL) remove the CMS UCM User ID or revoke the specific access privileges that are no longer required.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All personnel using or administrating the system are either CMS employees or direct contractors. As such all users are required to complete annual CMS Security Awareness Training and Privacy Act Training. In addition to the Security Awareness training, all UCM contractors are required to complete annual Data Security & Privacy Training and HIPAA Requirements training.

Describe training system users receive (above and beyond general security and privacy awareness training).

Not applicable.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

NARA Approved Disposition Authority: DAA-0440-2013-0001

Documents relating to Personal Identifiable Information (PII) and Protected Health Information (PHI) on providers and beneficiaries who have reported that their Medicare information has been compromised and suspects their Medicare information has been stolen through fraudulent methods.

DISPOSITION: Cutoff at the end of the calendar year of the completion of all legal activity. Destroy 7 years after cutoff.

NARA Disposition Authority: NC1-440-79-1/75/23/2B7 FROZEN--DO NOT DESTROY

Files accumulated as a result of allegations or complaints of program abuse or potential fraud by physicians and other providers of services pursuant to sections 206, 208, 1106, and 1107 of the Social Security Act. They consist of complaints from beneficiaries or other sources that are referred to district offices, regional offices, intermediaries, carriers, etc. Included are correspondence, forms, and other papers used in developing and investigating complaints, such as exhibits, copies of claims forms, bills, medical records, investigative reports, fiscal records, and other pertinent physician and provider records.

DISPOSITION: CMS Headquarters and Regional Offices
Place in inactive file after final action on the case. Cut off inactive file at the close of the calendar year in which final action was taken, hold 2 additional years, and then transfer to a Federally-approved records storage facility. Destroy after a total retention of 5 years.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Data is secured according to CMS Baltimore Data Center Security Standards and the CMS Acceptable Risk Safeguards (ARS).

Administrative controls include: Documented UCM System Security Plan, Contingency Plan, and Risk Assessment.

Technical Controls include: Resource Access Control Facility (RACF) in concert with DB2 (product name) security controls to limit access of UCM to authorized users, userids and passwords, RSA (product name) Tokens, firewalls, Virtual Private Networks (VPNs).

Physical Controls Include: guards, identification badges, key cards, closed circuit TVs.