# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

10/07/2016

### OPDIV:

OIG

### Name:

Data Warehouse (OIGDW)

**PIA Unique Identifier:**

P-8215280-039820

**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.**

Agency

**Is this a new or existing system?**

New

**Does the system have Security Authorization (SA)?**

Yes

**Indicate the following reason(s) for updating this PIA.**

**Describe the purpose of the system.**

OIGDW serves as an aggregation point for data feeds regarding analysis work on Medicare and Medicaid fraud, waste, and abuse. Data feeds include: CMS National Claims History File, Medicare Enrollment Database, National Provider Identifier Database. Also ingests death records from the SSA.

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

The information includes Medicare and Medicaid claims, provider, and beneficiary data. Drug, provider taxonomy, and geographical reference data, as well as fraud investigations data is also included.

- Name
- Email
- SSN
- DOB
- Mailing address

- Phone numbers
- Certificates (educational, licensing)
- Education records
- Taxpayer identifiers
- Medical records identification number
- Employment status
- OIGDW user name & password

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

The OIG Data Warehouse maintains an extract of Medicare paid claims data from the CMS National Claims History File sufficient to conduct the data analyses underlying OIG's audits, inspections, and investigations of the Medicare program. The OIG obtains this information under the authority of the Inspector General Act of 1978, 5 U.S.C. App. 3. The system also obtains information from other CMS systems - Medicare Enrollment Database and the National Provider Identifier database. Drug Pricing information is obtained from a variety of sources (third party vendors and CMS). We also collect information from the Social Security Administration (SSA) - records of deaths that have been reported to SSA. This file includes the following information on each decedent, if the data are available to the SSA: SSN, name, DOB, date of death, state or country of residence (2/88 and prior), ZIP code of last residence, and ZIP code of lump sum payment.

The information contained in the database documents paid claims information submitted by health care providers for inpatient, outpatient, home health, hospice, skilled nursing facility, physician and supplier and durable medical equipment. The information includes prescription drug event data and drug pricing data. The information also includes beneficiary and provider identification and program enrollment data. The information contained within contains the necessary data elements to retrieve source documentation from Medicare contractors and providers in the course of audits, inspections and investigations.

User credentials and passwords are collected by the system to authenticate users to their system access level.

**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

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Certificates

Education Records

Employment Status

Taxpayer ID

User credentials (user name/password)

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

Employees

Public Citizens

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

Vendor/Suppliers/Contractors

Patients

**How many individuals' PII is in the system?**

1,000,000 or more

**For what primary purpose is the PII used?**

The information is maintained for OIG internal use in support of audit, inspection, and investigative activities. However, information may be provided to entities outside the OIG where it is essential to conduct audit, inspection, and investigative activities. For example, PII may be selectively provided to a healthcare provider or Medicare contractor in order to obtain additional medical information essential to an audit, inspection, or investigation.

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

The OIG may also provide information to the Department of Justice to support an ongoing criminal investigation or court case.

De-identified PII may be used for testing purposes.

**Describe the function of the SSN.**

Identification and record summoning (this tracks provider system protocols). The SSN is only shared for appropriate/permitted law enforcement purposes.

**Cite the legal authority to use the SSN.**

Inspector General Act of 1978

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

Inspector General Act of 1978

**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.**

09-90-1000 Consolidated Data Repository

**Identify the sources of PII in the system.**

**Government Sources**

Other HHS OpDiv

State/Local/Tribal

Other Federal Entities

**Identify the OMB information collection approval number and expiration date**

N/A

**Is the PII shared with other organizations?**

Yes

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

**Within HHS**

Information may be provided to entities within HHS but outside the OIG where it is essential to conduct audit, inspection, and investigative activities.

**Other Federal Agencies**

The OIG may also provide information to the Department of Justice to support an ongoing criminal investigation or court case as described in the routine use section of the SORN. This information sharing activity is authorized by SSA § 1128C Healthcare Fraud Prevention Program.

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

N/A

**Describe the procedures for accounting for disclosures.**

OIG is developing measures to account for disclosures of PII from the system.

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

OIG does not collect the information from individuals - rather, the OpDIV uses information collected by CMS to further the audit, investigatory and criminal aspects of the OIG mission.

**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.**

Opting-out is not an option. OIG does not perform the information collection. OIG ingests the information collected under CMS programs.

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

OIG does not perform the data collection - any such notifications would be the responsibility of the CMS system from which OIG receives the data.

**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.**

The burden is on the entity collecting the information to provide channels for individuals to voice concerns regarding their PII. Upon notification from collecting entity, OIG will take all possible steps to ensure that once updated data is available, OIG systems reflect that information.

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

OIGDW System Owner intends to implement a Continuity of Operations Plan (COOP) for the system. System mirroring is planned after a database migration is complete. Service Level Agreements (SLA) are currently in place.

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

**Users:**

Conducts audits, evaluations and inspections, and investigations

**Administrators:**

Routine maintenance which is not possible without full access

**Developers:**

Database maintenance which is not possible without full privilege

**Contractors:**

Database and system maintenance provided by direct OIG contractors which is not possible without full privilege

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

OIGDW limits user access to those with a justifiable business need to gain access to system. Administrators and developers are granted access to maintain and update the system as needed.

**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.**

Access requests are reviewed by Administrators before users gain access to the OIGDW systems or PII held within. Access is granted based on business need.

**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.**

Annual Privacy Awareness Training is provided to all OIG users.

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

NIST-compliant role-based training is planned for users with escalated privileges or routine access to sensitive information.

**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.**

DAA-0468-2013-0010 - Destroy After 8 Years

NC1-440-79-1/75/23/2B7 - FROZEN (do not destroy)

440-79-1/8 - FROZEN (do not destroy)

NI-440-09-09 - Temporary, destroy 6 years after a case is closed or when no longer needed for Agency use, whichever is later

The information is updated periodically, at least semiannually, from current extracts from the CMS National Claims History Data Base. Previously extracted Medicare claims data is aged and deleted from the system when no longer required to support ongoing or planned audits, inspections, and investigations of the Medicare program.

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

The information is maintained on a centrally managed OIG computer system. Access is restricted by physical and computer-based access controls. Access is strictly limited to authorized OIG staff members via a two level authentication process. Users must be initially authenticated as valid OIG staff and are then authenticated to the Audit & Evaluation System by an independent second level authentication system. All computer files and printed listings are safeguarded in accordance with the provisions of the National Institute of Standards and Technology Federal Information Processing Standard 31, and the HHS Information Resources Management Manual, Part 6, "ADP Systems Security." Other security measures include guards to verify authenticity of ID badge and user identity, cipher locks on server doors, and CCTV monitoring of access to restricted areas.