US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/29/2016

OPDIV:

OIG

Name:

OIG Platform Services

PIA Unique Identifier:

P-2847277-485353

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)?

No

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

Describe the purpose of the system.

OIG Platform Services (OPS) is a centralized information system supporting OIG mission and administrative operations authorized by the Inspector General Act of 1978, 5 U.S.C. App 3. The system is maintained for the purpose of documenting, tracking, and reporting OIG administrative, audit, inspection, and investigative activities. It contains the Administrative Tracking Application (ATA), Office of Investigations (OI) Inspections Application, and Office of Evaluations and Inspections (OEI) Report Tracker.

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

General information is collected by all OPS systems
First and Last Names
System Username and Password
Date of Birth
Phone number
Email addresses

Home addresses
Social Security Number (SSN)
Employment information
Business partner names
Names of entities that individual is authorized to work for
Education information
States in which individual is licensed to (practice medicine, distribute Durable Medical Equipment (DME)…)
Legal documents
Vehicle identifiers
Certificates
Taxpayer ID
Name of OIG personnel assigned to case/task/project
Dates associated with activities on case/task/project
Web Uniform resource Locators (URLs)

Information particular to ATA:
Employment information
HHS ID
Emergency contact name/phone number (could be spouse/partner, parent, child, sibling, neighbor, etc.)

Information particular to the OI Inspections Application:
Names of OIG personnel
Names of Case Subjects
Photographic Identifiers
National Provider Identifier (NPI)

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

OPS maintains user credentials in order to administer the system and to enable system audits and non-repudiation. OPS currently contains the following three applications:

Administrative Tracking Application (ATA): provides a method for inputting, and then allowing access to secure, accurate and timely OIG employee administrative records.

OEI Report Tracker: provides management of the workflow of Office of Evaluation and Inspections (OEI) headquarters report processing.

OI Inspections: supports field office inspections conducted by Office of Investigations (OI). It facilitates the collection, storage, analysis, and retrieval of information and documents pertinent to the inspection process.

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

Photographic Identifiers

Vehicle Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Financial Accounts Info

Certificates

Legal Documents

Education Records

Employment Status

Taxpayer ID

NPI

URL

user credentials

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?

500-4,999

For what primary purpose is the PII used?

The information is used to further the audit, inspection, and investigative management activities fighting fraud, waste and abuse.

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

Administrative support for day-to-day operations.

Disclosure to other federal agencies as described in the System of Records Notices (SORNs).

Describe the function of the SSN.

SSN is used to unambiguously identify individuals involved in OIG audit, investigation, or administrative activities.

Cite the legal authority to use the SSN.

Privacy Act of 1974
Freedom of Information Act
E-government Act
Inspector General Act of 1978, 5 U.S.C. App 3
Federal Rules of Evidence (FRE)
Federal Rules of Criminal Procedure

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

OIG’s mission authorized by the Inspector General Act of 1978, 5 U.S.C. App. 3, as amended.

Pursuant to subsection (j)(2) of the Privacy Act, 5 U.S.C. 552a(j)(2), the Secretary has exempted the criminal investigative files of this system from the access, amendment, correction, and notification provisions of the Act, 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(3), and (e)(4)(G) and (h).
The civil and administrative investigative files are exempted from certain provisions of the Act under 5 U.S.C. 552a(k)(2). Pursuant to 45 CFR 5b.11(b)(2)(ii)(D), the files are exempt from the following subsections of the Act: (c)(3), (d) (1)-(4), and (e)(4) (G) and (H).

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.

Administrative Files, SORN 09-90-0076

Civil and Administrative Investigative Files of the Inspector General, SORN 09-90-0100

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Other

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Foreign

Other Federal Entities

Non-Governmental Sources

Public

Commercial Data Broker

Media/Internet

Private Sector

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

Case information may be shared with the OIG Audits and Evaluations teams. The information shared may encompass the entire case file, depending on the requirements of the individual request. The requests are often made to ensure that OIG efforts are not duplicated and the law enforcement activity is not compromised by inadvertent disclosure during the conduct of an audit or evaluation.

Other Federal Agencies

Case information may be shared with other law enforcement agencies, including U.S. Attorneys offices, state prosecutors, or any state or federal law enforcement agencies (including OIGs) with whom a joint investigative is being conducted as described in the SORN(s) routine disclosures.

State or Local Agencies

Case information may be shared with other law enforcement agencies, including U. S. Attorneys offices, state prosecutors, or any state or federal law enforcement agencies (including OIGs) with whom a joint investigative is being conducted as described in the SORN(s) routine disclosures.

Private Sector

As dictated by Federal regulations, some information (such as exclusions) is made available to the public via notification letter and by the public facing OIG website.
FOIA requests are public documents, we are required by Executive Order 12600 to provide a copy of the Freedom Of Information Act (FOIA) request when processing private sector records, i.e., Pfizer, Purdue, Johnson & Johnson.

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

Memorandum of Understanding (MOU) with Department of Treasury for Federal Do Not Pay database.

Describe the procedures for accounting for disclosures.

Disclosures in automated systems are tracked via audit logs. OIG is in the process of formalizing a mechanism for accounting for non-automated disclosures.

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

There is no process in place to notify individuals that their PII will be collected for law enforcement and audit functions, per exceptions in governing statutes. These regulations cover requests for investigative files by both complainants and potential targets. System users are required to provide unique username and passwords to allow system audits and to verify the authenticity of the user. No notice is provided other than to inform them that system access will not be granted without unique credentials.

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.

Hotline and other complainants are given the option of how much personal information they choose to provide. Investigative subjects or targets are not notified of the collection of information, because of the risks of evidence destruction and witness tampering. There is no option to opt-out of providing a unique user name to access the system - the user credential allows for authentication and non-repudiation of system activities logged by a unique user.

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

In such a circumstance the SORN will be updated and posted in the Federal Register and PIAs will be updated and re-posted as necessary. For the majority of OIG systems the exemption for law enforcement activities applies. For OIG system users creation of an account constitutes consent to provision of user credential PII and the unique user name is required for system auditing purposes and the OIG transition to full PIV-enabled single-sign on will minimize the opportunity for the loss/leakage of user name PII.

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.

This is only an option for non-law enforcement aspects of OIG activities. In these cases the External Affairs team fields the request and passes it along to the appropriate System/Business Owner.

For system users who have a concern regarding collection, use or disclosure of user credentials they may report to the appropriate system administrator who will escalate for an investigation as needed.

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

Information is input and maintained in investigative files by the case agent. As part of their duties, the information is required to be both up-to-date and accurate. Any discrepancies or errors identified can and will be corrected by the case agent. The proper maintenance of files and data accuracy are elements of the performance review process for OIG special agents.

For an individual who requests a correction to his Privacy Act information, OIG will follow the procedures documented in the Privacy Act regulation.

OIG has a process for periodic review of the privacy controls described in federal guidelines. The basic controls will be reviewed annually for each OIG system with a PIA. The remainder of the controls will be assessed once every three years, or when a major system change is made.

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

Users:

To execute the tasks supported by the system

Administrators:

Information technology support staff requires administrative access in order to support the operations and maintenance.

Developers:

Information technology support staff requires administrative access in order to support the operations and maintenance.

Contractors:

Direct contractors have access as required to perform assigned functions, including system maintenance, development and data inputs.

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

Access to OPS is restricted to authorized users. Those authorized users are identified by the business owners of the audit, investigative, evaluation and counsel systems, and are limited to special agents, investigative counsel, or investigative support staff within OI, auditors, evaluators.

Information particular to the OI Inspections Application:
Only authorized staff OI can see what is in the database. Access to the database is limited to IT direct contractors and inspectors who are added to the database for each particular inspection. The administrator has the ability to add and subtract inspectors to/from each new inspection that is loaded into the database. Information from the database, which could include those names, is shared with Office of Investigations executives and designated senior managers, and reports generated from the database are attached to final inspection reports that are sent to the senior manager of the region inspected.

OCIG personnel may also have access to the reports when necessary.

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.

Administrators for each system are expected to provide users with the role that enables them to perform their function with the least access necessary.

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.

Administrators are trained annually on PII and both the “need to know” and minimum necessary” standards. Access to systems and the information therein is expected to the provided in accordance with those guidelines. Annual security and privacy awareness training is mandatory for all OIG personnel and contractors. Role-based training on PII and system administration is provided to appropriate users (business owners, managers, system administrators).

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

Role-based training is required once every three years.

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.

OIG follows the HHS Policy for records management. Unique OIG records and disposition is documented in the following National Archive and Records Administration (NARA) approved record schedules:

OIG DAA-0468-2013-0008 - Permanent records transferred to NARA for archiving every 4 years once the most recent record in a 4 year block reaches 30 years old.

OIG DAA-0468-2013-0010 - Temporary files are destroyed 8 years after cutoff (end of fiscal year in which audit was closed); Permanent records transferred to NARA 5 years after cutoff.

OIG DAA-0468-2013-0011 - Temporary files are destroyed 7, 10 or 20 years after cutoff (end of fiscal year in which case was closed), depending on which sub-category the information falls under; Permanent files transferred to NARA 15 years after cutoff.

OIG DAA-0468-2013-0012 - Temporary files are destroyed 5 or 8 years after cutoff (end of fiscal year in which evaluation is closed); Permanent files transfer to NARA 15 years after cutoff
OIG DAA-0468-2013-0013 - Destroy 15 years after cutoff (the end of the fiscal year in which the case was closed).

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

Records and IT systems containing them are maintained in a restricted area and accessed only by authorized Department personnel. Access within OIG strictly limited to authorized staff members and is monitored. All employees are given instructions on the sensitivity of OIG files and the restrictions on disclosure. Access within OIG is strictly limited to management officials and employees on a need-to-know basis. All computer files and printed listings are safeguarded in accordance with the provisions of the National Institute of Standards and Technology Federal Information Processing Standards 199 and FISMA requirements, including physical security such as lock(s) of various types, closed circuit TV, security presence and other physical controls deemed appropriate. OIG systems can only be accessed using authenticated credentials by individuals intentionally granted access to each system.

Note: web address is a hyperlink.