US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/07/2016

OPDIV:

OIG

Name:

Corporate Management System (CorpView)

PIA Unique Identifier:

P-4288458-424682

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?

Yes

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.

CorpView consists of a group of logically related individual applications that conduct, document, and track audits, evaluations, and investigations regarding HHS programs and operations; document OIG reviews of allegations/complaints for HHS programs/operations; aid prosecutions in OIG investigations; maintain record of activities subject to investigations; report OIG investigation results to other departmental components for use in operating\evaluating programs and civil\administrative sanction imposition; and act as repository\source for information to fulfill reporting requirements of 5 U.S.C. App. 3 as mandated by IG Act of 1978. The system creates and saves unique user names and passwords.

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

General information collected by many systems
System user name and password
First/Last Names
Business Name

Addresses
Telephone numbers
Email addresses
SSN
Taxpayer ID
Name of OIG personnel assigned to case/task/project
Dates associated with activities on case/task/project
Organization an individual is associated with

Information particular to major sub-systems:

Correspondence Control Management System (CCM)
Responses to requests for information
Formal testimony
Rules and regulations
OCIG Subpoena Tracker
OI Region requesting subpoena
HHS program involved
Subpoena information
Cover letter, subpoena, subpoena attachment

OI Investigative Reporting and Information System
Criminal, civil, and administrative outcomes of investigations

OI Management Implication Report System
Recommendations to HHS divisions to reduce fraud, waste, and abuse.
Names, descriptions, and authorities of HHS programs

OI Evidence Tracking System
Individuals Medical records numbers
Computers/ hard drives- serial and model numbers
Cellphone serial and model numbers
Administrative and banking documents

OIG Advisory Opinion tracker
Name of requester
Fee estimates and invoice amounts

WebAIMS
Business partner names
Location information, including Internet address

OAS Headquarters Audit Report Tracking System (HARTIS)
OAS audit work products and related documentation
Draft and final audit reports
Memoranda and letters
Public summaries of restricted reports
OCIG legal opinions on audit matters
Meeting notes

Administrative and Civil Remedies Branch (ACRB) Case Tracker
OIG Case Number
Case/Claim Type

Qui Tam Compliant information
Docket Numbers
OIG Case Number Cross Reference
Project/Subject Type
Archive Accession Number and Box Number
Litigation Hold Status
USAO Jurisdiction
Contact Person’s Name, Phone, Address, Email and Participation Begin and End Date
Case/claim documentation, including status, updates, comments and OIG personnel assigned to the project
Self-Disclosure
US Attorney's Office (USAO) communications/determinations
Referral Source and notifications
Litigation Plan
Procedural History for case and appeals
Case Resolution documentation
Case status
Information on individuals referred for suspension or debarment
Information on Unilateral Monitoring programs
Emergency Medical Treatment and Labor Act (EMTALA) case/compliant information
Exclusion Opinion supporting information

OIG Corporate Data Transfer System
Pay rate
Pay period
Direct deposit information
Beneficiary information

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

The CorpView system is maintained to document, track, and report OIG's audit, inspection, and investigative activities. It also supports the day-to-day OIG administrative functions.

Investigative reporting subsystem (contains multiple applications): Maintains a record and documents outcome of OIG reviews of allegations and complaints received concerning HHS programs and operations; serves as a source for information necessary to fulfill OIG statutory reporting requirements.

Audit information subsystem (contains multiple applications): Maximizes staff resources and provides audit cost summary data; supports time and attendance functions; schedules and tracks training.

Correspondence Control Management (CCM): Tracks correspondence between Inspector General, Members of Congress, and others; responses to public inquiries, testimony and statements for Congress; press releases; rules and regulations created by OIG; internal memos and administrative policies, and reports.

FOIA Tracker: Manages FOIA requests.

OIG Internet: Website supporting availability of materials to public

OIG Intranet: Limited-access internal website

OIG SharePoint Portal: Internal OIG file sharing

OCIG Legal Review Tracker: Tracks status of items (complaints, self-disclosure, results of audits/investigations) submitted for legal review/comment.

OAS Flextraining System: Administers auditor-specific training.

OEI Management Information System: Tracks and reports on key evaluations activity, including milestones and due dates.

OIG Award System: Tracks OIG award nominations.

OCIG Case Tracker: Tracks status of case files as they run the legal review and workup process (supports audit and law enforcement mandates).

OCIG Subpoena Tracker: Automated system to track subpoenas (supports law enforcement mission).

OCIG Advisory Opinion Tracker: Tracks and manages advisory opinion requests.

OI Activity Reporting System: Tracks case-related investigator activities.

OI Investigative Reporting and Information System (IRIS): Automated case and workload management system.

OI Firearms Tracking System: Manages firearms information and training requirements.

OI Evidence Tracking System: Identifies, tracks and provides chain of custody for property/evidence collected during law enforcement activity.

OI Locator: Administration and calendaring application to provide centralized view of investigator resources.

OI Management Implication Report: Tracks Management Implication Report recommendations and status of implementing these recommendations

OAS Audit Information Management System: Produces information on in-progress, completed, and canceled audits.

Web Uniform Resource Locator(s) (URL): WebAIMS has URL fields that link to unrestricted final audit reports - final and draft - posted to the Internet.

OAS Headquarters Audit Report Tracking System (HARTIS): Tracks reports, memos and related under review by auditors.

OIG Corporate Data Transfer System: Allows administrators to access payroll and personnel data for administrative functions.

OIG Training Tracking System: Track, monitor and report employee training activities

OIG Budget Tracking System: Tracks commitments and obligations against budgeted allowances for OIG Components.

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

Driver's License Number

Mother's Maiden Name

E-Mail Address

Mailing Address

Phone Numbers

Financial Accounts Info

Certificates

Legal Documents

Education Records

Employment Status

Taxpayer ID

Web Uniform Resource Locator(s) (URL)

User credentials (username/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

How many individuals' PII is in the system?

100,000-999,999

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; as evidence in legal proceedings.

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).

Privacy Act of 1974
Freedom of Information Act
E-government Act
Federal Rules of Evidence (FRE)
Federal Rules of Criminal Procedure

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

Criminal Investigative Files of the Inspector General, HHS/OS/OIG, SORN 09-90-0003;

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

Other

Non-Governmental Sources

Public

Commercial Data Broker

Media/Internet

Private Sector

Other

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 Offices of Audits and Evaluations. 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

FOIA requests are public documents, we are required by EO 12600 to provide a copy of the 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.

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 logs.

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

In accordance with Freedom of Information Act (FOIA) and Privacy Act regulations that address the production and release of OIG records. These regulations cover requests for investigative files by both complainants and potential targets; responses are implemented pursuant to FOIA and the Privacy Act of 1974. 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.

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 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. Further, 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.

For investigative files, agents are trained and expected to maintain correct and up-to-date information.

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

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.

Others:

Access to CorpView 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.

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

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.

For the OCIG Subpoena Tracker: Administrator takes annual Privacy Awareness training.

For the OI Evidence Tracking System: Case agents and administrators.

For the FOIA Tracker: Access is to the MAIN FOIA database is restricted to only personnel assigned to the OIG FOIA office. Each component has a component version of the database with access provided by the FOIA officer only.

For the OI Firearms Tracking System: The authorized personnel for this database includes instructors and certain managers.

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.

Annual security and privacy awareness training is mandatory for all OIG personnel and all contractors, including direct 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 are 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 are 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. OIG systems can only be accessed using authenticated credentials by individuals intentionally granted access to each system.

Identify the publicly-available URL:

http://oig.hhs.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes