Privacy Impact Assessment for

Office of Inspector General Network (OIG-NET)

October 24, 2019

Contact Point
Gopala Seelamneni
Chief Information Technology Officer
Office of the Inspector General

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The Office of Personnel Management (OPM) Office of Inspector General (OIG) is an independent oversight office within OPM. The OIG NET General Support System is an information technology (IT) environment used to manage data in support of the office's core business functions. OIG NET stores information collected by OIG employees during audits, investigations, and evaluations. This Privacy Impact Assessment is being conducted because the information collected, maintained, or disseminate by OIG NET includes personally identifiable information.

Overview

The Office of Personnel Management (OPM) Office of Inspector General (OIG) is an independent oversight office within OPM. In accordance with the Inspector General Act of 1978, as amended, the OPM OIG conducts audits, investigations, and evaluations of OPM programs and the contractors that support these programs. The OPM OIG is a law enforcement agency that is involved in the civil and criminal prosecution of alleged violations affecting OPM's programs and operations, as well as administrative proceedings, as appropriate.

The OIG NET General Support System is an information technology (IT) environment used to manage data in support of the OIG's core business functions. Specifically, the OIG NET stores information collected by OIG employees during audits, investigations, and evaluations. The system also contains tools that allow OIG employees to view and manipulate the system's data for analysis. The information is used by OIG employees to evaluate the efficiency of OPM programs, to determine whether health insurance claim payments were made in accordance with applicable laws and regulations, and to detect fraudulent and/or criminal activity. The primary sources of information in the system include Claim data feeds, Ad-hoc claims data, employee-generated data, and Ad-hoc audit and evaluation document requests.

Claim data feeds are health insurance claims data feeds from insurance carriers that are automatically loaded to the system's Secure File Transfer

Protocol (SFTP) server on a monthly basis. This data includes medical claims, enrollment, pharmacy, and provider related information associated with the Federal Employees Health Benefits (FEHB) Program run by OPM. The FEHB Program is a coordination of managed competition through which employee health benefits are provided to civilian government employees and annuitants of the United States government. These files are stored as data sets and in conjunction with analytics tools are collectively referred to as the Health Claims Data Warehouse (HCDW).

Ad-hoc claims data is collected when auditors and investigators routinely request specific health insurance claims data from specific insurance carriers. OIG employees manually load this data to the OIG NET using one of several approved secure methods. Employee generated data is developed when OIG employees document interviews with the parties associated with an audit or investigation and store this information within OIG NET. Ad-hoc audit and evaluation document requests are also stored in OIG NET; OIG employees request a wide variety of documentation from audit/evaluation subjects to support findings and conclusions. OIG investigators may also store ad-hoc document requests in a separate system outside the scope of the OIG NET.

All information in OIG NET is stored on a centralized storage device where it can be accessed by authorized OIG employees using a variety of tools and applications, including the HCDW. OIG employees can use available tools to view, analyze, and manipulate the insurance claims data in the system. In addition, OIG auditors can use an audit management program to organize, track, and generate reports on data in support of specific audit engagements. The system also uses Active Directory to allow OIG Information Technology (IT) staff to manage access to the OIG NET environment and the various data and tools it contains. It is used to assign and manage the security policies of all components of the system including computer servers, network devices, applications, user workstations, printers, and copiers.

OIG IT staff also track the flow of sensitive information within OIG NET with a tool that continuously scans OIG NET to detect incoming and outgoing personally identifiable information (PII) or protected health information (PHI). The tool generates various reports and sends alerts to system

administrators. Additionally, OIG IT staff use another system tool to perform automated vulnerability scans of all of OIG NET's components.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The OPM OIG conducts audits, investigations, and evaluations of OPM programs and the contractors that support these programs pursuant to the Inspector General Act of 1978, as amended. The general authority for the OPM OIG to maintain records containing SSNs is provided by Executive Order 9397 as amended by Executive Order 13478, Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers (November 18, 2008).

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The OPM/CENTRAL-4 Inspector General Investigations Case Files SORN, the OPM/CENTRAL-18 Federal Employees Health Benefits Program Claims Data Warehouse SORN, and the OPM/GOVT-1 General Personnel Records SORN apply to information maintained in OIG NET.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes, the system security plan was created March 15, 2019.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. N1-478-08-001, OPM Inspector General Records.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information contained within OIG NET is not covered by the PRA. Records within the system are of Federal employees and contractors that are obtained from the agency files and interviews. The system does not collect

information directly from individuals; therefore the Paperwork Reduction Act (PRA) does not apply. In addition, the PRA does "not apply to the collection of information during the conduct of an audit, investigation, inspection, evaluation, or other review conducted by . . . any Office of Inspector General. . . ." 5. U.S.C. app. § 6(k).

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The following information about individuals is maintained in OIG NET components and applications in support of OIG's mission:

The Health Care Data Warehouse component maintains the following information about individuals: first name; last name; Social Security number; date of birth; gender; home address; names and genders of covered spouse and other dependents; FEHBP member ID number; Enrollee's employing agency; names of health care providers including health care providers debarred under 5 U.S.C. 8902a.; health care provider address; health care provider Taxpayer Identification Number (TIN) or identifier issued by a carrier; health care coverage information regarding benefit coverage for the plan in which the person is enrolled; health care procedure information regarding procedures performed on the individual; health care diagnoses in the form of ICD codes, and treatments, including prescribed drugs, derived from clinical medical records; provider charges, including amounts paid by the plan and amounts paid by the enrollee for the coverage, procedures, and diagnoses; and administrative information.

The Teammate application maintains the first name and last name of the medical provider being audited.

There are two File Storage Services. One contains the specific information collected about subjects of audits or investigations. This includes information about federal employees and annuitants, OPM contractors, and medical providers participating in the FEHBP. While the type and amount of PII collected depends on the objective and topic of the investigation or audit, this first File Storage Service includes: first and/or last name; Social Security

number (SSN) or other government issued identifier; physical identifying information (e.g., tattoo, birthmark); vehicle identifier (e.g., license place, VIN); driver's license number; residential address; personal phone numbers (phone, fax, cell); personal mailing address; personal e-mail address; business address; business phone number (phone, fax, cell); business e-mail address; medical record number; financial account information; birth, marriage, and/or death certificates; and legal documents or notes (e.g., divorce decree).

The second File Storage Service contains information maintained about OIG employees for internal human resources purposes. This maintains information about OIG employees and contractors for administrative and human resources purposes, including: first and/or last name; date of birth; place of birth; Social Security number (SSN); military, immigration or other government issued identifier; driver's license number; residential address; personal phone numbers (phone, fax, cell); mailing address; personal e-mail address; business address; business phone number (phone, fax, cell), and business e-mail address.

In support of OIGs internal administrative functions the Active Directory maintains the following information on OIG employees: name of the federal employee or contractor for user-account creation, permissions, and network logon credential purposes; physical and mailing addresses; telephone numbers; and email addresses.

2.2. What are the sources of the information and how is the information collected for the project?

The sources of information in the system include direct collection from the individual record subjects, complainants, or third parties with information pertinent to OIG investigative activities (including witnesses and other entities having some relationship with the record subject); the files of OPM offices and their systems of records; other Federal, state, and local agencies; non-government record sources, including commercial databases that provide public records search and link analysis capabilities; and FEHB insurance carriers.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

While OIG Net does not directly connect with any commercial or publicly available data sources, OIG investigative staff use commercial and publicly available data sources in the course of their investigative activities. These data sources may be used to obtain information that is used to corroborate evidence and to identify and locate potential subjects, witnesses, and record sources. The source of the information is generally noted when the incorporation of the information is recorded pursuant to standard OIG procedures regarding the evidential documenting of investigative activities.

2.4. Discuss how accuracy of the data is ensured.

The OIG staff reviews and validates subject information by comparing basic data, such as name, Social Security number, and date of birth and verifying the information with internal records. All collected information is subject to evaluation and scrutiny by OIG investigative staff and verified against information collected from other records sources. There are also built in audit logs to monitor disclosures and determine who had access during this time. These logs are checked regularly to ensure that the system is accessed appropriately. SSNs are also used to confirm identities of individuals pursuant to standard law enforcement procedures. SSNs may also be used to meet certain law enforcement matching requirements and where necessary to facilitate certain law enforcement requests.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information in the system will be inaccurate or incomplete, resulting in an adverse decision for the individual being investigated.

Mitigation: This risk is mitigated by requiring OIG investigative staff to adhere to standard investigative procedures whereby they validate information obtained against other record sources.

Privacy Risk: There is a risk that more information than is necessary to achieve the business function of the system will be collected and maintained.

Mitigation: This risk is mitigated by clear investigative processes and procedures to identify appropriate information and to evaluate the information collected for relevancy and accuracy. With respect to the OIG staff human resources information contained in the system, only the information necessary to meet appropriate human resources requirements should be collected and maintained.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

Information is maintained in this system in order to allow the OIG to meet its statutory responsibility to provide independent and objective oversight of OPM, including by conducting criminal, civil, and administrative investigations related to OPM programs and operations. Information collected and maintained in the system is used to detect and investigate activity constituting a potential violation of law, rule, or regulation; or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety; and to support the pursuit of criminal, civil, or administrative actions for such activities, as appropriate. Information is also used by OIG management to track, evaluate, and manage program operations, and as a basis for reporting investigative results and statistics internally and externally.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

OIG Net has search features which query by keyword-based algorithms and identifying data. However, none of these features are used to discover or locate predictive patterns or anomalies.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

Although no other program or office within OPM has direct access to OIG NET, some information contained and managed by the OIG NET is shared with other OPM programs in support of human resources and administrative operations and contracting procurement operations. These OPM offices and

programs include security, human resources, Help Desk, Equal Employment Opportunity, and procurement. The information provided to them may include name, SSN, date of birth, mailing address, phone number, and email address.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that an authorized person may access the information for an unauthorized purpose and that PII may be accessed or used inappropriately or in a manner not consistent with the original intent of the collection.

Mitigation: This risk is mitigated by limiting access and documenting disclosures. Reports from the system are used internally by OIG management. All employees who are authorized to access are required to have as a pre-requisite certain OIG training, including an ethics briefing. Users are further required to sign specific rules of behavior to access OIG Net and other IT resources.

Privacy Risk: There is a risk that individuals who do not have a need to know the information contained in the system will access and use the information.

Mitigation: This risk is mitigated by limiting access according to user roles and work assignments and reviewing audit logs to ensure that unauthorized users have not accessed the system. The risk is further mitigated through the use of physical and IT protections designed to limit access to only those with a need to know.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Notice is provided through this PIA and the SORNs identified in section 1.2. Notice is also provided with respect to certain categories of information collected from system users, including administrative and personnel (support) records.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Most of the information in OIG Net is considered investigatory material, compiled for law enforcement purposes in connection with the administration of the merit system. When information is obtained directly from the record subject, individuals may have the opportunity to decline to provide information. OIG criminal investigators are trained as to investigative subjects' rights and obligations when responding to OIG inquiries, and the OIG has policies in place to ensure that subjects are made aware of those rights, as appropriate.

In instances where information is obtained by the OIG from other record sources (including witnesses, commercial or publicly available databases, and Federal systems of records) the individual generally is not provided the opportunity to consent or object to the OIG's collection. Providing individuals additional specific notice at the point of collection of information could negatively impact the investigative activities of the OIG by, for example, alerting the subjects of criminal investigations as to the Government's prosecutorial strategies or the nature of evidence collected.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware that their information is collected and maintained by OIG NET.

Mitigation: This risk cannot be fully mitigated because the OIG's investigation mission may be compromised. However, the risk is mitigated as appropriate when there is direct communication with subjects and through the publication of this PIA and the SORNs referenced in Section 1.2.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

OIG currently follows record retention schedule (N1-478-08-001), which covers most OIG records. The following are standard times for which information in OIG NET is retained: health care provider debarment files are retained for 15 years after termination or most recent action; FEHBP carrier

records are retained for 3 years; audit files are retained for 10 years after the audit is closed; audit final report files are retained for 20 years after the audit is closed; investigative case files are retained for 15 years after the case is closed; investigation complaints are retained for 5 years after cutoff date; agent notes on investigations are retained for 10 years after cutoff date; legal advisory files are 1retained for 0 years after cutoff date; and litigation case files are retained for 20 years after termination of a case. For those records that are not covered by N1-478-08-001, OIG is working with OPM's record's officer to establish an appropriate schedule with NARA. Until that schedule is approved, affected records may not be destroyed or deleted.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by OIG staff being trained appropriately and then following the established retention schedule and documented guidance from NARA. OIG staff are directed to dispose of any/all background investigation records in accordance with its agency-specific NARA regulations, and consistent with documented agreements between the external agencies and OIG. This risk is not currently mitigated for those records that have not yet been scheduled; however, OIG is working to mitigate the risk associated with those records by taking steps to establish an appropriate records schedule.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. No external entities have direct access to OIG NET but information is shared with external entities where necessary to meet the mission needs of OIG. For example, information is shared with Department of Justice (DOJ) and other law enforcement partners as appropriate to facilitate the OIG's investigative activities or in order to comply with reporting requirements. Information is also shared, as appropriate, with other Federal, state, and

local agencies (including other Federal Offices of Inspectors General) pursuant to joint investigations involving OPM programs and operations, or where the OPM OIG becomes aware of an indication of a violation or potential violation of law falling within the jurisdiction of the agency.

Sharing occurs through both electronic and non-electronic means, as determined by the particular circumstances of the information sharing. Any information sharing from OIG NET is consistent with the statutory responsibilities set forth in the Inspector General Act of 1978, which authorizes the audit, investigation, and evaluation of OPM programs and operations as well as the collection of related information.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Any disclosure of Privacy Act-protected information is only done consistent with the purposes stated in the relevant SORN identified in Section 2.1 and pursuant to an applicable routine use or other Privacy Act exception.

6.3. Does the project place limitations on re-dissemination?

Any disclosure of information from OIG NET may be accompanied by a notice advising against further release of the information without the prior authorization of the OPM OIG.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

Disclosures of information are recorded as part of OIG's standard investigative procedures which require staff to timely document and track case activity.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in OIG NET will be shared with a third party and used or disseminated for a purpose that is not consistent with the purpose for which it was collected.

Mitigation: This risk is mitigated by implementation of internal guidance regarding the appropriate release of information and by limiting releases to scenarios where it is necessary to facilitate OIG mission-related activities. This risk is further mitigated by limiting OIG employee access to only that information that they need to know to fulfill their business functions.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

There is limited access to many of the records contained in OIG NET because they have been exempted from the access provisions of the Privacy Act, 5 U.S.C. § 552a(c)(3) and (d). Individuals wishing to request access to any non-exempt records pertaining to them should contact the system manager identified in the applicable SORN listed in Section 1.2. Individuals requesting access must also comply with OPM's Privacy Act regulations regarding verification of identity and access to records (5 CFR part 297).

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

There is limited opportunity to amend many of the records in OIG NET because they have been exempted from the amendment provision of the Privacy Act at 5 U.S.C. § 552a(d). Individuals wishing to request amendment of any non-exempt records pertaining to them should follow the process outlined in the applicable SORN listed in Section 1.2. Individuals requesting amendment must also comply with OPM's Privacy Act regulations regarding verification of identity and amendment of records (5 CFR part 297).

7.3. How does the project notify individuals about the procedures for correcting their information?

Individuals are notified about the procedures for correcting information through the SORNS identified in Section 1.2 and through publication of this PIA.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have the opportunity to access their information or amend inaccurate information contained in OIG NET.

Mitigation: This risk cannot be completely mitigated for all records in OIG NET because providing individuals the opportunity to access or amend certain information could negatively impact the investigative activities of the OIG by, for example, alerting the subjects of criminal investigations as to the Government's prosecutorial strategies or the nature of evidence collected.

Further, the accuracy or relevance of information obtained during the course of an investigation may not be readily apparent at the time of collection. Accordingly, allowing the premature amendment of information could inhibit or detrimentally affect the OIG's capacity to detect unlawful activity. However, this risk is partially mitigated by the publication of instructions in this PIA, and in the SORNs listed in section 1.2, to inform individuals about how to request access to and amendment of their records, notwithstanding that certain records in this system have been exempted from the access and amendment provisions of the Privacy Act.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

The OPM OIG Information Assurance Branch reviews audit logs in order to ensure appropriate use of the information in OIG NET. Users are granted only the permissions they need to accomplish their function, and cannot view data that is not pertinent to their role. This includes the ability to identify specific records each user can access. In general users are assigned roles based on their group, and have permissions inherited from that group. This typically includes only being able to view information and files relevant to the group they are part of.

OIG also conducts third party audits and OIG NET has automated tools to indicate when information is possibly being misused. Improper access, and anomalous logon patterns and behavior on OIG NET are all reported via automated tools.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OIG employees are required to complete OPM's annual IT Security and Privacy Awareness training, and the OIG releases an annual IT Rules of Behavior that all staff sign. Specific offices within the OIG go through their own training to ensure that privacy is maintained. For example, the database team is provided with PHI and PII training and the Office of Audits and the Office of Investigations complete database access protocol training.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

User access is based on express permission and access to information is limited to those OPM OIG employees with a need to know the information in the performance of their duties. Access is limited solely to OIG employees, who are granted access to the system and assigned roles by system administrators. Users' access is further limited within the system to information pertaining to their assigned duties during the pendency of those duties. Firewalls and data encryption methods ensure the data can be accessed by authorized OIG personnel only.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The OIG does not have any information sharing agreements, nor is access to OIG NET granted to non-OIG personnel. Any new uses of the information, memoranda of understanding, information sharing agreements, or provisions of access would be reviewed by OIG senior level management, to ensure that the contemplated change aligns with the OIG's mission, that necessary technical safeguards are in place, and that all legal requirements are met.

Responsible Officials

Norbert Vint
Acting Inspector General
Office of the Inspectors General
Office of Personnel Management

Approval Signatures

Signed copy on file with the OPM Chief Privacy Officer

Kellie Cosgrove Riley,
OPM Chief Privacy Officer
Office of Personnel Management