US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/07/2016

OPDIV:

OIG

Name:

Audit Work System (TeamMate)

PIA Unique Identifier:

P-1850603-749670

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.

TeamMate is an Audit Management System (AMS) supporting the OIG's audit responsibilities authorized by the Inspector General Act of 1978, 5 U.S.C. App. 3 that provides a centralized data repository for project planning and enterprise risk evaluation; project, time, and expense documentation; audit recommendation and risk follow-up; and centralized reporting for management. The system is maintained to increase the efficiency and productivity of the audit process by automating working paper preparation, internal review, report generation, and retention. The system also captures time and expenses charges, status of recommendation implementation, employee personnel data, staff planning data, and enterprise risk management data. The system utilizes the commercial software product, TeamMate, to manage and integrate working papers prepared with various standard office automation products.

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

Social Security Number of beneficiaries from medical records

Date of Birth of beneficiaries from medical records

Name of beneficiaries from medical records and of system users

Photographic Identifiers of beneficiaries from medical records, of targets from investigative assists, and of users if they uploaded to their user profile

E-Mail Address

Mailing Address of beneficiaries from medical records, of auditees from working papers, and of users

Phone Numbers of beneficiaries from medical records, of auditees from working papers, and of users

Medical Records Number of beneficiaries from medical records

Medical Notes from beneficiaries' medical records

Financial Account Info from auditee financial records

Certificates from auditee records to document staff training

Legal Documents of auditees from working papers and of targets from investigative assists

Education Records from auditee records

Device Identifiers from auditee records

Employment Status from auditee records

Taxpayer ID from auditee records

User Login Name and password for system users

Hire date of system users

Title of system users

Grade of system users

Direct and indirect time charged from timecards of system users

Reimbursable rate from timecards of system users

Medical records of beneficiaries

Medical claims of beneficiaries

IT system records from auditee records and audit working papers

Documentation pertaining to audits and other projects

Documentation pertaining to grand jury investigations

Financial records from auditee

Opinions of OIG staff related to work

Communication between staff members related to work

Communication with auditee and HHS Operating Divisions (OpDivs) related to work

Recommendation implementation results from OpDivs related to audit findings

Non-working time recorded from system user time cards

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

The type of audit information collected, maintained and/or stored by TeamMate may include information on OIG staff, time charged to project, computer login information such as user credentials including usernames and passwords, information relating to audits which may include: medical records, medical claims. The system also may contain IT system records, assorted documentation pertaining to audits and related projects, documentation pertaining to grand jury investigations, financial records, internal (interim) OIG staff communications, communication with auditee and HHS Operating Divisions (OpDivs), recommendations, and implementation guidance.

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

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Certificates

Legal Documents

Education Records

Device Identifiers

Employment Status

Taxpayer ID

User Credentials: User Login Name and 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?

TeamMate is used to conduct/support audit and related investigations (if any). Any PII in the system is used for those purposes and for OIG administration of auditor functions.

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

Some of the PII related to user accounts is used for testing and training. Completed projects may be accessed by other approved staff for research. Use of PII collected in individual projects depends of the objective of the work. The system only stores the information and does not analyze it.

Describe the function of the SSN.

The SSN is the basis of the Health Insurance Claim Number (HICN) used to identify beneficiary in receipt of services from an audited entity and while the TeamMate system does not use the SSN, it is located on all claim data and is part of medical records.

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.

5 U.S.C. Appendix § 4(a) and 6(a) (Inspector General Act of 1978) authorizes the Inspector General to conduct, supervise, and coordinate audits relating to the programs and operations of the Department and to have access to all documents or other material available to the Department which relate to its programs and operations.

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Foreign

Other Federal Entities

Non-Governmental Sources

Public

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

For purposes of resolving recommendations, collection of debts and overpayments, and debarment and suspension.

Other Federal Agencies

Other Federal Agencies for purposes of required peer review; Department of Justice for advice.

State or Local Agencies

For referrals, litigation, and alternative dispute resolution.

Private Sector

To public or private entities when necessary to obtain other information related to the audit; To contractors and consultants when hired for expertise in completion of audit work.

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

OAS requires all experts, consultants, or other OAS contractor employees/third parties with access to OAS information to execute a confidentiality agreement.

Describe the procedures for accounting for disclosures.

Disclosures are approved by Office of Counsel for the Inspector General on an as-needed basis.

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

Not applicable. In most cases OIG is not the original collector of the data. If it is, OIG is exempt per 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.

The civil and administrative investigative files are exempted from certain provisions of the Act per subsections (c)(3), (d) (1)-(4), and (e)(4) (G) and (H).

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.

Individuals are not provided the option to object to the collection of their information since it is normally collected from HHS systems which have previously performed the original collection. If OIG collects data it is exempt per the provisions cited above.

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

Apart from system users (employees), we do not notify or obtain consent from individuals whose PII is in the system when major changes occur to the system since we cannot identify every specific instance of PII and in most cases OIG is not the original collector of the information. System users are notified by mass email of major system changes.

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.

Individuals (OIG employees) are directed to contact the Chief Information Security Officer (CISO) if they believe their PII has been inappropriately obtained, is incomplete or inaccurate, or is being misused. Staff are informed of the proper procedures to follow in these circumstances during security and privacy training, which they are required to complete annually. Non-employees who wish to report an incident use the FOIA/Privacy Act reporting process. The individual at OIG who manages the FOIA/Privacy Act reports will direct the issue to the appropriate system owner, system administrator or other personnel to investigate and take appropriate action.

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

The TeamMate Centralized System is hosted at the OIG data centers, which includes a back-up location to ensure no loss of data/operations occurs in the event of an outage at the primary data center. To ensure an effective and viable contingency planning capability, periodic training, testing, and exercises is conducted on TeamMate components. This process will range from exercising parts of the Contingency Plan (e.g., notification phase) to full-scale tests of the entire TeamMate recovery and reconstitution process. Individual projects are reviewed by assigned managers to ensure data integrity, accuracy, and relevancy. OAS policies/protocol ensure availability of records (disaster recovery/continuity of operations planning). Internal Quality Control reviews are performed annually on samples of projects to ensure OAS policies and procedures are followed.

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

Users:

Users (OIG employees with a non-administrative role in the system) need access to PII related to their assigned projects and for management reports. Non-OIG staff may be granted access to TeamMate audit files with the explicit, express authorization of the cognizant Regional Inspector General for Audit, Assistant Inspector General for Audit, or OAS senior management.

Administrators:

Administrators have access to PII while setting up users and troubleshooting system errors.

Contractors:

Direct contractors operate on behalf of the agency and use the agency’s credentials when doing so.

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

Access is provided by the TeamMate Admin Team based on approval from OAS Audit Planning and Implementation (API) after the user has completed ethics training. Access is limited to those with an operational need to access the information. System administrators, developers, and contractors only access PII with approval from the API Director. Unpaid interns are not given access to system. Level of access depends on bona fide need.

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.

The system makes extensive use of roles, rights, and privileges to restrict access to PII. User login identifies the user and provides access to the system, then the user is further restricted by access to modules, and ultimately restricted by roles within each module. Only a select few administrative users have access to all the data.

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 users receive annual training on privacy awareness, ethics, records management, and information systems security awareness.

They are also required to read the Rules of Behavior for Use of HHS Information Resources and sign the accompanying acknowledgments. Awareness also comes from issued guidance stating that system data is not distributed to outside entities without written authorization from the API Director.

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

Users receive training on how to operate the system and are provided with a handbook for reference. Role-based training will be provided for all users who routinely access sensitive information in OIG systems.

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.

The records retention schedule is National Archives and Records Administration (NARA) records schedule number DAA-0468-2013-0010 which states to destroy 8 years after cutoff. Cutoff is at end of fiscal year in which audit is closed (audit recommendations are resolved).

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

The database and OIG servers are located within secured buildings. Appropriate physical security controls have been implemented at all locations - these may include access badges, security guards, closed-circuit television, and/or cipher locks. Logical controls which minimize the possibility of unauthorized access, use, or dissemination of the data in the system are in place. Access to the database is further controlled by system authentication and system role and team settings which strictly limit TeamMate access to authorized staff members.

Files in TeamMate are encrypted. 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."