US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/31/2024

OPDIV:

NIH

Name:

NIH OD GSS_DPI TeamMate T4

PIA Unique Identifier:

P-1690853-043434

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Internal Flow or Collection

Describe in further detail any changes to the system that have occurred since the last PIA.

TeamMate Audit is being updated to reflect the added collection of HHS ID numbers.

Describe the purpose of the system.

TeamMate Audit is a comprehensive audit management system designed to help auditors and audit department leadership manage all aspects of the audit process. TeamMate allows the Department of Program Integrity (DPI) to identify risk and create assessment reports, schedule projects and allocate resources, capture time and expenses, track audits and issues, and create and manage audits via an advanced electronic working papers database. NIH uses this software to track allegation and contact information and meet requirements of digital compliance.

In addition, the system will be a repository and tracker of NIH enterprise risk data and documentation

of high priority internal control risk assessment selected senior leadership.

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

TeamMate Audit collects, stores, and shares personally identifiable information (PII) to manage the audit process, including: Name, E-Mail Address, Phone Numbers, Date of Birth, employment status, HHS ID number, foreign activity, and Mailing Address. Additionally, some supporting documents may contain social security numbers (SSNs) and Taxpayer IDs but the collection of both is not a function or part of the system and there is no direct storage of either within the system. All efforts are made to redact them.

NIH employees log into the system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user names and passwords (user credentials) and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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

TeamMate Audit is a comprehensive audit management system designed to help auditors and audit department leadership manage all aspects of the audit process. TeamMate allows the Department of Program Integrity (DPI) to identify risk and create assessment reports, schedule projects and allocate resources, capture time and expenses, track audits and issues, and create and manage audits via an advanced electronic working papers database. NIH uses this software to track allegation and contact information and meet requirements of digital compliance.

In addition, the system will be a repository and tracker of NIH enterprise risk data and documentation of high priority internal control risk assessment selected senior leadership.

TeamMate Audit collects, stores, and shares personally identifiable information (PII) to manage the audit process, including: Name, E-Mail Address, Phone Numbers, Date of Birth, employment status, HHS ID number, foreign activity, and Mailing Address. Additionally, some supporting documents may contain social security numbers (SSNs) and Taxpayer IDs but the collection of the both is not a function or part of the system and there is no direct storage of either within the system. All efforts are made to redact them.

NIH employees log into the system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user names and passwords (user credentials) and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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
Employment Status
Foreign Activities
Taxpayer ID
HHS ID number

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?

500-4,999

For what primary purpose is the PII used?

The primary purpose of PII is to manage the audit process. TeamMate Audit is a comprehensive audit management system designed to help auditors and audit department leadership manage all aspects of the audit process. TeamMate allows NIH personnel to identify risk and create assessment reports, schedule projects and allocate resources, capture time and expenses, track audits and issues, and create and manage audits via an advanced electronic working papers database.

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

Not applicable

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

Section 402(b)(1) of the Public Health Service Act, 42 U.S.C. 282 (b)(1)

45 C.F.R. 74.53(e)

Federal Acquisition Regulation, 48 C.F.R. Sections 15.209(b)(1) and 52.215-2

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.

09-90-0003 Criminal Investigative Files of the Inspector General

09-25-0213 Administration: Employee Conduct Investigative

09-25-0223 NIH Records Related to Research Misconduct Proceedings, HHS/NIH

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

Identify the OMB information collection approval number and expiration date

Not applicable

Other HHS OpDiv
State/Local/Tribal
Foreign
Other Federal Entities
Non-Governmental Sources
Public
Media/Internet
Private Sector

Is the PII shared with other organizations?

Yes

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

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

not applicable; terms and conditions through point of purchase

Describe the procedures for accounting for disclosures.

The system owner works in conjunction with the Business Owner and the NIH Privacy Officer to account for disclosures. Disclosure must be compatible with the purpose for which the records were collected.

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

The program website fully notifies all interested parties of the process, including the collection, use, and storage of PII.

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.

There is no opt-out option. The collection of PII is required to use the system and also participate in the audit process.

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

Any major system changes that would impact individuals and the collection of their PII would be sent via email. The system also has the capacity to generate and send individual communications when needed for individual notification.

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.

If an individual has concerns about the use of their PII, they may contact the system administrator.

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

There is no formal periodic review of PII used in the system as the use of PII is limited and specific to each case.

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

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

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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.

The NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness).

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

Stakeholders with elevated role-based privileges may also participate in regular simulation and desktop training exercises. TeamMate maintains comprehensive instructional documents and best practices on their enterprise site.

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.

Records are retained and disposed of under the authority of the NIH Records Control Schedule, as follows:

Item 02-001: Official case files of construction, renovation, endowment and similar grants. Cut off annually following completion of final grant-related activity that
represents closing of the case file (e.g., project period ended). Destroy 20 years after cutoff. (DAA-0443-2013-0004-0001)

Item 02-005: Official Case Files of Applications and Awards, Appeals, and Litigation Records for Grants, Cooperative Agreements, and Other Transaction Activities. Cut off annually following completion of final award-related activity that represents closing of the case file (e.g., end of project

period, completed final peer review, litigation or appeal proceedings concluded). Destroy 30 year(s) after cutoff. (DAA-0443-2019-0008)

Item 02-003: Animal welfare assurance files. Cut off annually following closing of the case file. Destroy 4 years after
cutoff. (DAA-0443-2013-0004-0003)

Item 02-004: Extramural program and grants management oversight records. Cut off annually. Destroy 3 years after cutoff. (DAA-0443-2013-0004-0004)

Item 01-002: Intellectual property records consisting of intramural research records and project documentation that supports patents or inventions rights. Cut off annually after the patent is filed. Destroy 30 years after cutoff. (DAA-0443-2017-0002-0001)

Item 08-102: Records for internal control risk assessments. Destroy no sooner than 6 years after the project, activity, or transaction is completed or superseded, but longer retention is authorized if needed for business use. (DAA-GRS-2013-0002-0007)

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

Administrative: Administrators are trained on using Teammate Audit and how to set up role-based privileges. Users participate in desktop training exercise. Standard Operating Procedures are in place for the use and handling of PII within the system.

Technical: NIH Personal Identity Verification cards are required to access the system. Additionally, IAM is used to authenticate and authorize users accessing the system. IAM maintains its own PIA, including all legal authorities documented.

Physical: Physical controls are handled by the cloud provider and include limiting access to servers by having them locked in secure rooms.