US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/26/2024

OPDIV:

NIH

Name:

Technology Information Management System

PIA Unique Identifier:

P-1454372-748409

The subject of this PIA is which of the following?

Minor Application (child)

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?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

The Technology Transfer Center (TTC) Technology Information Management System (TIMS), is a life cycle tracking system for the technology transfer agreements negotiated by NCI TTC. The system monitors various types of agreements and documents related to agreements, which includes:
Material Transfer;
Confidential Disclosure;
Clinical Trial;
Cooperative Research and Development;
Letter of Collection;
Memorandum of Understanding;
Employee Invention Reports;
Patent Filings; and
License Agreements.

The system also includes document management, access to Outlook, and access to Outlook's Task

Manager.

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

The information TIMS collects, maintains and disseminates is business contact information, including name, title, employer name, work address, work phone, and work email address. This information is required for the negotiation and execution of technology transfer agreement.

When an individual enters negotiations with the National Cancer Institute (NCI), they send their information by email to the NCI employee conducting the negotiation (system user), who then enters the data into the system. Previously, information may have been supplied by mail or fax but such methods are not used anymore.

The Internet is used solely for the purposes of verification. For example, when distinguishing between two contacts sharing the same name, NCI may utilize a search engine to corroborate their respective employers.

Users log in to this system using 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. IAM Services collects unique user credentials and stores them in an encrypted format. 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.

The Technology Transfer Center (TTC) Technology Information Management System (TIMS), is a life cycle tracking system for the technology transfer agreements negotiated by NCI TTC. The system monitors various types of agreements and documents related to agreements, which includes:
Material Transfer;
Confidential Disclosure;
Clinical Trial;
Cooperative Research and Development;
Letter of Collection;
Memorandum of Understanding;
Employee Invention Reports;
Patent Filings; and
License Agreements.

The system also includes document management, access to Outlook, and access to Outlook's Task Manager.

The information TIMS collects, maintains is business contact information,including name, title, employer name, work address, work phone, and work email address. This information is required for the negotiation and execution of technology transfer agreement.

When an individual enters negotiations with the NCI, they send their information by email to the NCI employee conducting the negotiation (system user), who then enters the data into the system. Previously, information may have been supplied by mail or fax but such methods are not used anymore.

The Internet is used solely for the purposes of verification. For example, when distinguishing between two contacts sharing the same name, NCI may utilize a search engine to corroborate their respective employers.

Users log in to this system using 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. IAM Services collects unique user credentials and stores them in an encrypted format. 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.

Name
E-Mail Address
Mailing Address
Phone Numbers
Title
Employer Name

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Personally identifiable information (PII) is used by TIMS to identify and track individuals representing external entities entering into agreements, licenses, invention, or patents with NCI.

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

N/A

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

Public Health Service Act. (42 U.S.C. 241, 242, 248, 281, 282, 284, 285a-285q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101)

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.

09–90–0067, Invention, Patent, and Licensing Documents Related to Inventions By Public Health

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Hardcopy
Email
Government Sources
Within OpDiv

Identify the OMB information collection approval number and expiration date

TIMS does not collect information from the general public; therefore, it is not subject to the

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

Paperwork Reduction Act (PRA).

Is the PII shared with other organizations?

No

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

Individuals are notified that their personal information will be collected during the process of negotiating agreements or licenses between the government and outside entities the contacts work for or while preparing invention and/or patent applications the individuals are part of.

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.

Entering into an agreement, license, invention, or patent with the NIH is voluntary.

However, if an external entity chooses to enter into an agreement, license, invention, or patent they may not opt-out of the collection of PII. They must supply a representative's business contact information including name, mailing address, e-mail, and phone number.

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

All individuals are notified and give consent that their business information is collected for purposes of transacting technology transfer agreements. No processes are currently in place to notify individuals should major changes to data use occur. However, should a major change occur, the records would be amended at which point the individuals would have the option to consent to the 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.

During negotiations, the business representative has time to review or change any information or voice any concerns about the information. Before final execution of any agreement, license or patent application, the representative must review any and all documentation and indicate their acceptance with their signature. During the entire life cycle of the agreement, should the individual have a concern about their information, they would contact the NCI Negotiator to inform them of their concerns. The NCI Negotiator would address and resolve the concerns.

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

Data is monitored and reviewed during the life of the agreements, licenses, inventions or patents. The NIH IT Privacy Program requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected systems.

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.

Supervisors contact the data administrator when a new employee joins the program. Together the supervisor and the data administrator assess the employee based on their role and duties; only those employees whose duties include the creation, monitor or review of agreements, licenses, inventions or patents are then granted access to the system by the data administrator. Database administrators are not granted access to the data files as their role is only to maintain the server in which the data is stored.

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.

There are 2 security groups in the system which control access to the data in the system; 1) Security Group 1 has access to all the data 2) Security Group 2 has access to only the data necessary to create, edit or monitor the records in the system. The data administrator determines to which group users will be assigned based on their roles and duties. The number of users in Security Group 1 is very limited.

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 manage or operate NIH applications or systems must attend complete security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management, and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

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

None.

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 Intramural Records Retention Schedule.

Item 04-101, Employee Invention Reports (EIRs) and Patent Applications: These records consist of invention descriptions and associated documents submitted by scientists to technology development coordinators for review of patentability or transfer by other means; and U.S., Patent Cooperation Treaty {PCT) and foreign patent applications and related documents including evaluations, work orders, and Cooperative Research and Development Agreements {CRADA) with a reported CRADA Subject Invention. Disposition: Temporary; Cut off following expiration, lapsing, withdrawal or abandonment of all issued patents, and patent applications within an associated patent family; or

unpatented inventions when not associated with licensable or available licensed research material. Destroy 6 year(s) after cutoff or when no longer needed for business purposes occurs, whichever is later.
DAA-0443-2016-0002-0001

Item 04-102, License Agreement, CRADA and Other Technology Transfer Agreement Records - Executed Agreements with Financial Terms: These records include license agreements, CRADAs, and other Technology Transfer Agreements. Disposition: Temporary, Cut off at expiration or termination of the License, CRADA or Technology Transfer Agreement. Destroy 6 year(s) after cutoff or when no longer needed for business purposes occurs, whichever is later.
DAA-0443-2016-0002-0002

Item 04104,License Agreement, CRADA and Other Technology Transfer Agreement Records - All Other Agreements without Financial Terms and All Other Non-executed Agreement Applications: These records include license agreements, CRADAs, and other Technology Transfer Agreements. Disposition: Temporary; Cut off at: 1) termination of the Agreement or at the expiration of the Agreement term or the Confidentiality term, whichever is longer; or 2)Confirmation that the activities under the Agreement are no longer continuing; or 3) When the Application/Agreement is withdrawn, the negotiations are terminated, or the license application is denied and there is no appeal. Destroy 3 year(s) after cutoff or when no longer needed for business purposes occurs, whichever is later.
DAA-0443-2016-0002-0004

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

Administrative Controls:
The system conducts or performs management oversight activities, security awareness and training, separation of duties for personnel administering the system, and isolates development test instances of the system. In addition, all personnel with access to the system are required to abide by the HHS and NIH Rules of Behavior upon completing security awareness training as a new hire and then annually.

Technical Controls: The database server is hosted by NCI/NIH behind a firewall, which limits access to only NCI/NIH employees. Further access to the system is controlled by security groups; only users added to a security group have access to the system through NIH Active Directory. Only NCI/NIH users with a valid user name and password in AD can access TIMS database and the password policy is enforced through NIH's active directory policy. When a user is deemed to no longer need access, the user is removed from the security group. When users are transferred or terminated, their NIH account gets deleted which automatically removes the user from the security group.

Physical Controls: The server resides in the Shady Grove Data Center and access is limited to the data center technical personnel only. All NIH personnel are issued badge/PIV cards for identification purposes.