US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/26/2025

OPDIV:

NIH

Name:

Take Your Child to Work

PIA Unique Identifier:

P-1608186-135540

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

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

The PIA has been updated to meet the requirements of Executive Order - Defending Women From Gender Ideology Extremism And Restoring Biological Truth To The Federal Government.

Describe the purpose of the system.

Take Your Child to Work (TYCW) event is hosted jointly by Office of Research Services (ORS) and The Office of Equal Opportunity and Diversity Management (OEODM). The website allows NIH Staff to view activities and register their children (age, sex, grade, name, and phone) for activities and print schedules.

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

Parents register their children in the TYCW system using their NIH badge. TYCW Database will collect information regarding child's name, sex, age and emergency contact information (parent's name, work phone, personal cell phone, and email) for this event only. Parent information is pulled from the NIH Enterprise Directory (NED). NED maintains its own Privacy Impact Assessment (PIA),

including all legal authorities documented.

Users log in to this system using the NIH Identity, Credential, and Access Management (ICAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of ICAM 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 ICAM Services collect unique user names and passwords (user credentials) and stores them in an encrypted format. The ICAM 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.

Take Your Child to Work (TYCW) event is hosted jointly by Office of Research Services (ORS) and The Office of Equal Opportunity and Diversity Management (OEODM). The website allows NIH Staff to view activities and register their children (age, sex, grade, name, and phone) for activities and print schedules.

Parents register their children in the TYCW system using their NIH badge. TYCW Database will collect information regarding child's name, sex, age and emergency contact information (parent's name, work phone, personal cell phone, and email) for this event only. Parent information is pulled from the NIH Enterprise Directory (NED). NED maintains its own Privacy Impact Assessment (PIA), including all legal authorities documented.

Users log in to this system using the NIH Identity, Credential, and Access Management (ICAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of ICAM 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 ICAM Services collect unique user names and passwords (user credentials) and stores them in an encrypted format. The ICAM 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
Phone Numbers
Personal cell phone numbers will be for emergency contact and are not required
Age of child; not date of birth
Sex of child

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

Employees
Public Citizens
Childrens names

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Data is shared with application administrators to assign employees' children for different activities during TYCW day and Division of Police so they can have records of children on campus.

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.

5 U.S. Code Sec. 301 and 302.

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

No

Identify sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OD

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

Not Applicable. An OMB collection approval number is not needed as the TYCW only requires the PII of federal employees and direct contractors for internal use only.

For members of the public (children of employees), no OMB collection numbers are needed because NIH is not soliciting information. Data of children are voluntarily given so that they can participate in TYCW activities.

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.

For information pulled from NED as a source system, NED notifies individuals that their PII will be collected during the time of entering into a business relationship with NIH. NED maintains its own PIA and all legal authorities are documented.

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 option for individuals to opt-out of the collection of of their PII. The information is needed to register children for different activities during TYCW Day. The information will also be shared with the Division of Police for safety reasons. If an individual wishes to not give their information, they cannot participate in the program.

For information information pulled from NED as a source system, NED notifies individuals that their PII will be collected during the time of entering into a business relationship with NIH. NED maintains its own PIA and all legal authorities are documented.

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

Consent is given during the registration process when parents of the children sign up electronically to participate.

For information information pulled from NED as a source system, NED obtains consent during the time of entering into a business relationship with NIH. NED maintains its own PIA and all legal authorities are documented.

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 with concerns that their PII has been inappropriately obtained may contact the TYCW business owner at the provided email on the registration form and on the TYCW website.

For information information pulled from NED as a source system, individuals can contact their servicing administrative officer or make updates to their own account. NED maintains its own PIA and all legal authorities are documented.

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

For data pulled from NED, periodic audits and reviews are done by system administrators. Data collected during registration is only used for that year's TYCW day and there are no reviews after that day and are destroyed after 1 year per the records retention schedule. NED maintains its own PIA, including all legal authorities documented.

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.

Access is based on role of person and the need to use or have access to the system. All requests for access go through the system administrator.

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 according to 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).

N/A

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 maintained within TYCW are destroyed one year after the business is ceased in accordance with NARA record retention schedule:

NIH Records Schedule 10-507; Records of non-mission related internal agency committees with a disposition authority of: DAA-GRS-2016-0016-0003.

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

Administrative Controls: The system administrator grants access based on the role of person and their need to use or have access to the system. An overview of the event, rules, and registration details are maintained by the system administrator and available for NIH employees to view.

Physical Controls: The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.