US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/31/2024

OPDIV:

NIH

Name:

NIBIB Training Grantees Meeting (TGM)

PIA Unique Identifier:

P-3483268-647866

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

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

The web application was converted from hypertext markup language (HTML) to the Drupal format, and is now hosted in the Acquia cloud.

Describe the purpose of the system.

Names and email addresses are collected in order to process login accounts by sponsors of the Clinical Care annual meeting. There is no open registration process, however, if a user forgets their password, there is reset feature that requires the user to enter their username or email address.

Each training session also displays the name and email address of the coordinator to contact for additional information or questions.

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

Name, email address and username are collected in order to process login accounts by sponsors of the Clinical Care annual meeting. There is no open registration process, however, if a user forgets their password, there is reset feature that requires the user to enter their username or email address.

Each training session also displays the name and email address of the coordinator to contact for additional information or questions.

Administrators and developers requiring access to the site log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 collects unique user credentials and stores them in an encrypted format. The IAM Service is 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 NIBIB TGM website lists the agenda of upcoming training sessions. Accounts are provided as requested by sponsors of the meeting.

Name, email address and username are collected to process login accounts. There is no open registration process, however, if a user forgets their password, there is reset feature that requires the user to enter their username or email address.

Each training session also displays the name and email address of the coordinator to contact for additional information or questions.

Administrators and developers requiring access to the site log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

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
Username
passwords

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The personally identifiable information (PII) is used to create a user account for access to the site.

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

Name or e-mail address can be used to recover passwords.

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

Section 301 of the Public Health Service Act, describing the general powers and duties of the Public Health Service relating to research and investigation (42 U.S.C. 241).

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.

09-25-0014 Clinical Research: Student Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OMB

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

N/A

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 specifically provide their information in order to create an account for registration. If they don’t provide it, they can't register.

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.

Submission of the information is voluntary. If they choose not to submit the information, they are not able to access the site, register, or reset their password.

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

In the event of a major change, the email address will be used to contact individuals.

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 may email info@nibib.nih.gov or contact the NIH Senior Official for Privacy at Privacy@mail.nih.gov.

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 NIH Information Technology (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. Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy.

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 to personally identifiable information (PII) is assigned to personnel based upon current job responsibilities. The system uses specific login information to assign permissions/user roles which is considered PII.

Administrators and developers log in to the site using NIH IAM Services which maintains its own unique PIA, with all legal authorities documented.

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.

According to NIH policy, all personnel who use NIH applications must successfully complete security awareness training annually. 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).

Web Developers and Privileged Users require additional training specific to their roles and responsibilities.

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 Retention Schedule.

Item06-601 - Non-mission employee training program records.
Non-mission employee training program records.
Exclusion: This item does not cover ethics-related training. Ethics training is scheduled by RSS Item

06-604 (General Records Schedule (GRS) 2.6, Item 020).
Records about planning, assessing, managing, and evaluating an agency's training program:
plans, reports and program evaluations
organizational and occupational needs assessments
employee skills assessments
employee training statistics
notices about training opportunities, schedules, or courses
mandatory training tracking and reporting files
logistics and coordination documents
Authorization, Agreement and Certification of Training (SF-182) and similar records registration forms, employee attendance records syllabi, presentations, instructor guides, handbooks, and lesson plans reference and working files on course content other course materials, such as presentations and videos student, class, or instructor evaluations Disposition: Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use. DAA-GRS-2016-0014-0001

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

Physical Controls: IT hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentications must be used for access. File integrity and auditing software are employed on hardware.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these sites use privileged and separate accounts for administrative access.

Note: web address is a hyperlink.