US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/28/2025

OPDIV:

NIH

Name:

NIGMS Meeting Registration System (MREGS 3.0)

PIA Unique Identifier:

P-3316352-308073

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?

Yes

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 National Institute of General Medical Sciences (NIGMS) Meeting Registration System (MREGS) has been enhanced to accommodate virtual and hybrid (virtual and in-person) meetings. MREGS now allows an unlimited number of registrants to register for a single meeting.

The following data fields have been added to MREGS version 5.0;
Time Zone
Meeting Type – Added virtual and hybrid meeting types to existing physical meeting type.
Virtual Meeting Details – Open text box where meeting organizers can insert additional details about a meeting such as a meeting link.
Session Type – Added virtual and hybrid meeting types to existing physical meeting type.

A fourth channel was created in MREGS for HHS/Office of the Assistant Secretary for Health

(OASH) and a service level agreement (SLA) was established.

Describe the purpose of the system.

The National Institute of General Medical Sciences (NIGMS) Meeting Registration System (MREGS) is a tool to facilitate the promotion and administration of meetings and conferences that are open to the public.

MREGS consists of three modules: a Public Site module, a Meeting Management module, and a User Management module.

The Public Site module is the public-facing portion of MREGS where meeting details are displayed, and registrants can register for meetings (open and available to the public).

The Meeting Management module is used to create and manage meetings (internal administration).

The User Management module is used to add users to the system and assigned channels and roles for access to the meeting management module.

There are four channels (instances) of the MREGS system to support NIGMS, National Institute of Neurological Disorders and Stroke (NINDS), Fogarty International Center (FIC), and HHS/Office of the Assistant Secretary for Health (OASH). Each channel is owned by the channel owner and the user administrators who manage groups and role assignments through user management. Any information collected within each channel is only accessible to the members of that channel. It is then further limited to only the organizer and facilitators of a specific meeting (i.e. meeting organizers/facilitators can only see information for the meetings they've created or manage). The MREGS Information Technology (IT) support (NIGMS' Service Desk) has read-only access to all channels for support purposes.

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

MREGS collects, maintains, and shares information about meeting dates, time, time zone, meeting type, location, agenda, meeting session topics, session type, speaker's name, custom content tab (open text field primarily used for biosketch) and meeting registrants contact information (name, degree designation, institution/organization, position, address, email, phone number).

The system provides a list of registrants with their contact information to generate attendee badges. It also provides a list of registrants who are on a waiting list for a meeting session and registrants who have cancelled registration for a meeting session or meeting.

Lastly, the system allows meeting administrators to generate session roster reports (can include any information collected during registration (meeting type, registration, name, address, e-mail, phone, position, and title) and an abstract listing report (name, title, abstract description, and organization).

Users log in to this 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 collects unique user credentials and stores them in an encrypted format. The IAM Services is an essential service which facilitates and governs network access to various resources.

Center Information Technology (CIT) limits HHS users access by the department field in their NIH Lightweight Directory Access Protocol (LDAP) record. Users are restricted by the department field. Both login avenues are coordinated through the NIH login IAM Services group. The NIH login is for

NIH users, and Federated login is used for OASH.

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

The NIGMS MREGS is a tool to facilitate the promotion and administration of meetings and conferences that are open to the public.

MREGS consists of three modules: a Public Site module, a Meeting Management module, and a User Management module.

There are four channels (instances) of the MREGS system to support NIGMS, NINDS, FIC), HHS/OASH. Each channel is owned by the channel owner and the user administrators who manage groups and role assignments through user management. Any information collected within each channel is only accessible to the members of that channel. It is then further limited to only the organizer and facilitators of a specific meeting. The MREGS IT support has read-only access to all channels for support purposes.

MREGS collects, maintains, and shares information about meeting dates, time, time zone, meeting type, location, agenda, meeting session topics, session type, speaker's name, custom content tab and meeting registrants contact information (name, degree designation, institution/organization, position, address, email, phone number).

The system provides a list of registrants with their contact information to generate attendee badges, a waiting list for a meeting session, and registrants who have cancelled. Lastly, the system allows meeting administrators to generate session roster reports and an abstract listing report.

Users log in to this system using the NIH Identity, Credential, and Access Management IAM Services which maintains its own unique PIA on record, including all legal authorities documented.

CIT limits HHS users access by the department field in their NIH LDAP record. Users are restricted by the department field. Both login avenues are coordinated through the NIH login IAM Services group. The NIH login is for NIH users, and Federated login is used for OASH

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
Institute/Organization, Education, Virtual Meeting Details, Conference/meeting information, Attendee's Position
Title

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?

100,000-999,999

For what primary purpose is the PII used?

The information is used to publicize and administer meetings and conferences.

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

There are no secondary uses.

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

5 U.S.C. 301, 305; 21 U.S.C. 301 et seq.; 31 U.S.C. 1115(b)(6); 40 U.S.C. 11313; 42 U.S.C. 201 et seq.; 44 U.S.C. 3101; E.O. 11583; E.O. 13571.

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.

09-90-1901 HHS Correspondence, Customer Service, and Contact List Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Other HHS OpDiv

Non-Government Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

For HHS OpDiv under MREGS that require OMB clearance, the facilitator will evaluate the program and request the OMB Control No: 0925-0740 Conference, Meeting, Workshop, Registration and Challenges Generic Clearance (OD). Expiration 09-30-2025

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.

NIGMS establishes Service Level Agreements (SLAs) with each component that owns an individual channel of MREGS.

Describe the procedures for accounting for disclosures.

The following language is included in all MREGS Service Level Agreements (SLAs): MREGS data will be used and/or accessed in compliance with relevant, statutory, regulatory, and NIH privacy policies.

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 website privacy notice includes a statement that PII is optional and collected voluntarily. Users can decline to provide PII, however, they will not be able to register for a meeting or conference.

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.

Users can decline to provide PII, however, they will not be able to register for a meeting or conference.

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

There will be no substantive changes to data uses. Information is collected in order to administer conferences and meetings. There is no further use of PII. However, if a major change occurs, the meeting coordinators can utilize the system to contact individuals to notify them and obtain consent.

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 chooses to include personal information, it is voluntary. Should individuals have concerns or need to update their information, they may contact the specific meeting owner (whose name is listed in MREGS) or contact MREGS technical support (as listed on the MREGS external site). In addition, they can contact the NIH Privacy Office 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 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.

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.

Access to PII is assigned to personnel based upon current job responsibilities. An NIH IAM Systems account login is required to gain access to the stored PII 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.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security and privacy awareness training. Training is completed on the http: //irtsectraining.nih.gov site with valid NIH credentials.

OASH users must abide by NIH policy as well as HHS requirements for information security, privacy awareness, records management, emergency preparedness, and HHS Rules of Behavior.

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

Administrators 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.

Item 11-502 Customer/Client Records.
Customer/client records. Distribution lists used by an agency to deliver specific goods or services. Records include:
contact information for customers or clients
subscription databases for distributing information such as publications and data sets produced by the agency
files and databases related to constituent and community outreach or relations
sign-up, request, and opt-out forms

Disposition: Delete when superseded, obsolete, or when customer requests the agency to remove the records. DAA-GRS-2017-0002-0002

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

Physical Controls are administered by Amazon Web Services. MREGS data is stored in the NIGMS DataMart which is hosted on an Amazon Web Services (AWS) data center cloud solution. The AWS cloud data center is located in geo-redundant facilities throughout the world.

Technical Controls: Technical Safeguards include restricting files using secure socket layer encryption, a two-factor authentication and role-based access controls.

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

Identify the publicly-available URL:

https://mregs.nih.gov/

(Users can see meetings listed under the table of contents if the meeting is active/public for each channel. The meeting registration link used for meeting registrations is always unique to that particular meeting).
Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null