US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/10/2024

OPDIV:

NIH

Name:

Council Member Website

PIA Unique Identifier:

P-2580456-311798

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.

This validation is intended to refresh content. There have been no substantive changes since the last Privacy Impact Assessment (PIA).

Describe the purpose of the system.

The National Institute of Child Health and Human Development (NICHD) Council Member Website (CMW) is specifically designed to provide an external facing site for NICHD's Advisory Council Members, providing them with online access to Council-related meeting and grant application assignment information. The site is also used by specific authorized extramural staff.

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

The CMW provides access to a repository of information to support the NICHD Advisory Council. Information collected, maintained, and shared through the extranet site includes Advisory Council meeting notes, meeting agendas, NICHD grant applications, Council Member task assignments, and action items.

The type of personally identifiable information (PII) the system will collect, maintain and/or share inlcudes Name, E-Mail Address, Phone Numbers, Mailing Address, and Employment Status of Advisory Members and NICHD grant requestors.

Information collected, maintained, and shared through the site includes Advisory Council meeting notes, meeting agendas, NICHD grant applications, Council Member task assignments, and action items.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique PIA on record, with all legal authorities documented. The purpose of the IAM 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 collects unique user credentials and stores them in an encrypted format. The IAM 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 Council Member Website is comprised of servers and software to provide an extranet site with restricted access to NICHD Advisory Council Members and authorized NICHD extramural staff. Information collected specifically applies to the conduct of NICHD Advisory Council meetings and Council Member tasks.

Information collected, maintained, and shared through the site includes Advisory Council meeting notes, meeting agendas, NICHD grant applications, Council Member task assignments, and action items.

PII collected, maintained and/or shared includes Name, E-Mail Address, Phone Numbers, Mailing Address, and Employment Status of Advisory Members and NICHD grant requestors.

Those requiring access to this system 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
Mailing Address
Phone Numbers

Employment Status

Advisory Council meeting notes, meeting agendas, NICHD grant applications, Council Member task assignments, and action items.

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

Employees

Public Citizens

No

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

PII is used for the administration of grant funding.

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

There is no secondary use for which the PII will be used.

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

42 USC 241 and 282

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

No

09-25-0036 Extramural Awards and Chartered Advisory Committees (IMPAC 2), Contract

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

OMB Number: 0925-0001 - expiration 01/31/2026

OMB Number: 0925-0002 - expiration 01/31/2026

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.

There are no specific Information Sharing Agreements (ISA) nor Memorandums of Understandings (MOU) between the CMW information system and the HHS other Federal Agencies. The sharing of NIH grant requesting and funding information agreements are established, reviewed, and maintained at the OPDIV level, not the system level.

Describe the procedures for accounting for disclosures.

The procedures for accounting for disclosures for NIH grant information are developed, maintained, and conducted at the OPDIV level not the system level. The CMW has no process to account for disclosures.

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 required to enter the information themselves through the OPDIV maintained website that also displays the Privacy Act Statement and explains what, why, and how personal information is shared and maintained.

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 process for the collection or use of their PII because PII is required to uniquely identify grant applicants, and to track and award funding to grantees. If individuals apply for funding, they must provide PII to identify themselves on the grant application.

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

System administrators will email individuals when major changes occur to the system that are deemed to necessitate notification and consent from those individuals whose PII is in the system.

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 contact the NICHD Privacy office, the NIH Senior Official for Privacy at Privacy@nih.gov; or email the Grants Information staff at GrantsInfo.od.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.

For PII that comes from NIH grant information, the OPDIV maintains their own processes and procedures for periodic reviews of PII and maintains its own PIA, including all legal authorities documented.

Individuals that have PII in the system may change or correct their grant application information (PII) using a specific process outlined on the https://grants.nih.gov website.

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.

The principles of least privileged access are applied. The system uses roles and each role has different access levels. The default role has the least privilege. Approval is needed to change a user's role.

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.

PII collected is available to authorized users and administrators of the system in accordance with the role they are authorized and assigned.

Council Members are limited to only the PII that pertains to the Council Member's area of expertise for the conduct of Council Member tasks, including grant funding decisions.

CMW Administrators have access to only the amount of PII needed to allow them to test and review data integrity, availability, accuracy, and relevancy.

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 attend security awareness training every year. There are five categories of mandatory information technology (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).

System owners, manager, administrators and operators are required to take role-based training.

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 02-004 - Extramural Program and Grants Management Oversight Records.
Item E-0004: Extramural program and grants management oversight records
These records are generated during the administration and execution of extramural program activities. This schedule item is intended to capture all extramural program and grants management records that are not part of an official case file (Item 0001 or 0002) or animal welfare assurance file (Item 0003). These records support the operations, compliance, reporting, and oversight functions of the NIH Extramural Program and the financing of research endeavors with the purpose of ensuring scientific integrity and public accountability of the NIH extramural research portfolio. Extramural program and grants management oversight records are consolidated under one common temporary retention item.

Disposition: Cut off annually. Destroy 3 years after cutoff. DAA-0443-2013-0004-0004

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

Physical Controls: The IT hardware used to host protected information is located in a secured datacenter facility at the Bethesda Data Center. 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 authentication 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 systems use privileged and separate accounts for administrative access. Access to source data files is strictly controlled by files staff. Records may be removed from files only at the request of the System manager or other authorized employees. Access to computer files is controlled by the use of registered accounts onlyl