US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/30/2025

OPDIV:

NIH

Name:

CRSS Bioethics Fellowship Application

PIA Unique Identifier:

P-5522100-474484

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?

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.

There have been no changes since the last update. Assessment is being updated to reflect new Point of Contact and authorization date.

Describe the purpose of the system.

The Clinical Center Bioethics Fellowship Application provides a method for applicants to apply for 4 to 6 fellowships for bioethicists' training.

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

Information collected when creating an application include: Name, mailing address and email address.

Once created, applicants may upload, delete and manage their supporting documents which may include: personal demographic and historical biographical information, academic information, writing

samples, coursework, Curriculum Vitae (CV) and resumes, and letters of recommendation. The web-based application provides program administrators the ability to search, sort and edit applications by several fields including, but not limited to, name, school, city, state, zip code, application status, application submission date.

Users requiring access 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 collect unique usernames and passwords (user credentials) and stores them in an encrypted format. The 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 Clinical Center Bioethics Fellowship Application provides a method for applicants to apply for 4 to 6 fellowships for bioethicists' training.

Information collected when creating an application include: Name, mailing address and email address.

Once created, applicants may upload, delete and manage their supporting documents which may include: personal demographic and historical biographical information, academic information, writing samples, coursework, Curriculum Vitae (CV) and resumes, and letters of recommendation. The web-based application provides program administrators the ability to search, sort and edit applications by several fields including, but not limited to, name, school, city, state, zip code, application status, application submission date.

Users requiring access 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 collect unique usernames and passwords (user credentials) and stores them in an encrypted format. The 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
Education Records
Employment Status
Resume/CV, demographic and historical biographical information, letters of recommendation

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

Public Citizens

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The Clinical Center Department of Bioethics uses the information to grant admission to selected applicants for the bioethicists' training opportunity.

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

Once a candidate has been selected, the personally identifiable information (PII) is used to contact them.

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

The legal authority to operate and maintain this Privacy Act records system is 42 U.S.C. §§ 241, 248, 282 and 284

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

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

0925-0698, expiration date 06/31/2026

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.

The application process is initiated and driven fully by each applicant. The individuals, therefore, are giving NIH notice that they wish to provide their personal information so that they may be considered for a place in the program.

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.

This is a voluntary application process. Opting out of collection and use of PII would prevent the applicant from consideration.

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

All applicants are notified of information practices. Major changes would not occur to this system as it is single-purpose and has a specific Office of Management and Budget (OMB) number that correlates to its one, single function.

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.

A Privacy Rights Complaint Form is available to individuals when they believe that their PII has been inappropriately used or disclosed. The Clinical Center's Privacy Office will review the complaint and respond to the concern within 30 business days. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC Privacy Officer.

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 PII is kept solely to evaluate an applicant's suitability. The PII would fall out of date with every new application period since resumes and academic activity are likely to change. No effort is made to ensure accuracy since applicants who are rejected would have to re-apply every year. PII submitted each year is not archived.

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

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.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles. Authentication with NIH Personal Identity Verification (PIV) card will occur at time of login to the NIH Network. System owners are responsible for creating the proper security groups within their systems with the applicable permissions for group members to enforce least privilege.

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 awareness training. 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).

Application specific, one-on-one peer training, is provided as needed.

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.

07-204, System access records; Systems requiring special accountability for access. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use)DAA-GRS-2013-0006-0004).

06-118, Special hiring authority program records. Destroy 2 years after hiring authority closes but longer retention is authorized if required for business use (DAA-GRS-2014-0002-0016).

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

Physical Controls: The information technology (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 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.

Identify the publicly-available URL:

https://bioethicsapps.cc.nih.gov/bioethicsApp/

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?

No

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