US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/16/2025

OPDIV:

NIH

Name:

NIMHD GSS: Portfolio Analysis Tool (PAT)

PIA Unique Identifier:

P-8932222-519776

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.

There have been no changes since the last assessment was done.

Describe the purpose of the system.

The Portfolio Analysis Tool (PAT) provides the National Institute on Minority Health and Health Disparities (NIMHD) with the ability to track and administer data for research applications and funded projects as well as identify funding redundancy and improve efficiency. It also provides access to reports, data and analyses of NIMHD research activities, including information on NIMHD expenditures and the results of NIMHD supported research. The system is designed to interface with the National Institutes of Health (NIH) Information for Management, Planning, Analysis, and Coordination (IMPAC) II module, which is part of the eRA (not an acronym) system via the NIMHD Datamart. eRA maintains its own privacy impact assessment.

PAT provides NIMHD with the following broad functionalities:

Project referral and tracking for preliminary branch assignments
Scientific coding support and maintenance (automated & manual)
Automatic pending records notification
Record search retrieval and full record detail display
Standard and customized report generation
Workload summary and project history tracking
Reference data maintenance
Data freeze for end of Fiscal Year (FY) reporting

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

PAT does not collect personally identifiable information (PII) directly from individuals and the PII is not the primary focus of PAT's portfolio management functions. PAT is designed to interface with the NIH IMPAC II module, which is part of the eRA system, which maintains its own unique privacy impact assessment (PIA)) via the NIMHD Datamart to collect data and information to include selected PII. The process to notify and obtain consent from individuals whose PII is in the source system is a part of the NIH standard application process for Principle Investigators, grantees, and direct contractors who are conducting research on behalf of NIH and NIMHD.

Through these systems, PAT will collect, maintain, or share user profile data; data related to research applications and funded projects (grants and contracts); and foreign site and funding data related to funded projects. The user profile data will be used to authorize PAT access and assign PAT system roles to users. The research applications and funded projects data will be used to track, monitor, and manage NIMHD related research applications and funded projects through their lifecycle.

User profile data includes Name, User Name, NIMHD email address, Phone Number, Begin Year (Year user profile activated), End Year (Year user profile inactivated) Roles (All PAT roles assigned to user).

Research application and funded project data includes Project Number, Application Class, Application Identification (ID),
Type Code, Activity Code, Institute/Center (IC), International Classification of Diseases (ICD) code, Serial Number, Support Year, Contract modification number, Sub-Project ID, Fiscal Year
Common Account Number (CAN), Request for Application (RFA) / Program Announcement (PA) Number, Branch, Program
Program Officer (PO) Initials, Program Class Code (PCC), Project Title, Coder Name, Principal Investigator (PI) Name
Coding Status, Intramural Branch.

Foreign site and funding data includes Country Code, Country Name, City, Postal Code, Institution Name, Percent and dollar amount funded by foreign site.

Users log into PAT 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 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 Portfolio Analysis Tool (PAT) provides the National Institute on Minority Health and Health

Disparities (NIMHD) with the ability to track and administer data for research applications and funded projects as well as identify funding redundancy and improve efficiency. It also provides access to reports, data and analyses of NIMHD research activities, including information on NIMHD expenditures and the results of NIMHD supported research. The system is designed to interface with the National Institutes of Health (NIH) Information for Management, Planning, Analysis, and Coordination (IMPAC) II, module, which is part of the eRA (not an acronym) system via the NIMHD Datamart. eRA maintains its own privacy impact assessment.

PAT provides NIMHD with the following broad functionalities:
Project referral and tracking for preliminary branch assignments
Scientific coding support and maintenance (automated & manual)
Automatic pending records notification
Record search retrieval and full record detail display
Standard and customized report generation
Workload summary and project history tracking
Reference data maintenance
Data freeze for end of Fiscal Year (FY) reporting

PAT does not collect personally identifiable information (PII) directly from individuals and the PII is not the primary focus of PAT's portfolio management functions. PAT is designed to interface with the NIH IMPAC II module, part of the eRA system (a source system which maintains its own unique privacy impact assessment (PIA)) via the NIMHD Datamart to collect data and information to include selected PII. The process to notify and obtain consent from individuals whose PII is in the source system is a part of the NIH standard application process for Principle Investigators, grantees, and direct contractors who are conducting research on behalf of NIH and NIMHD.

Through these systems, PAT will collect, maintain, or share user profile data; data related to research applications and funded projects (grants and contracts); and foreign site and funding data related to funded projects. The user profile data will be used to authorize PAT access and assign PAT system roles to users. The research applications and funded projects data will be used to track, monitor, and manage NIMHD related research applications and funded projects through their lifecycle.

User profile data includes Name, User Name, NIMHD email address, Phone Number, Begin Year (Year user profile activated), End Year (Year user profile inactivated) Roles (All PAT roles assigned to user).

Research application and funded project data includes Project Number, Application Class, Application Identification (ID),
Type Code, Activity Code, Institute/Center (IC), International Classification of Diseases (ICD) code, Serial Number, Support Year, Contract modification number, Sub-Project ID, Fiscal Year
Common Account Number (CAN), Request for Application (RFA) / Program Announcement (PA) Number, Branch, Program
Program Officer (PO) Initials, Program Class Code (PCC), Project Title, Coder Name, Principal Investigator (PI) Name
Coding Status, Intramural Branch.

Foreign site and funding data includes Country Code, Country Name, City, Postal Code, Institution Name, Percent and dollar amount funded by foreign site.

Users log into PAT 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 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
Phone Numbers
User name, IC, Begin/End Year, Role(s)
Country Name, Country Code, City, Postal Code, Institution Name
Project Number, Application Class, Application ID, ICD Number, CAN, Intramural Branch, PO Initials,

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

Employees
Public Citizens
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The primary use of PII is to authorize users and assign the user roles in the PAT application. The use of Principal Investigator (PI) personally identifiable information (PII) is to track and monitor research applications and funded projects throughout their lifecycle.

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

None

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

Section 301 of the Public Health Service Act, describes 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.

09-90-0024, HHS Financial Management System Records

09-25-0225, NIH Electronic Research Administration (eRA) Records (NIH eRA Records)

09-25-0216, Administration: NIH Electronic Discovery

Identify the sources of PII in the system.

Government Sources
Within OpDiv
Non-Governmental Sources
Public

Identify the OMB information collection approval number and expiration date

OMB # 0925-0001 Expiration Date:1/31/2026
OMB # 0925-0002 Expiration Date: 1/31/2026

OMB # 0925-0361 Expiration Date: 1/31/2026
OMB # 0925-0689 Expiration Date: 4/30/2025

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.

There is currently no Memorandum of Understanding (MOU) or Information Sharing Agreement (ISA) in place.

Describe the procedures for accounting for disclosures.

Except for those disclosures that are necessary to carry out NIMHD portfolio management functions, the PAT project team will maintain an accounting of disclosures of PII. The accounting:

Will contain the date, nature, and purpose of the disclosures and the name and address of the entity to whom the disclosure is made;

Be retained for at least three (3) years after the disclosure, or the life of the record, whichever is longer; and

Be available to NIMHD, or the person or entity who is the subject of the record, upon request.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

PAT is not the source system. eRA is the source system and maintains a process in place to notify individuals when their information will be collected. eRA maintains its own PIA.

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.

PAT is not the source system. eRA is the source system and maintains processes for individuals to opt-out. eRA maintains its own PIA.

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

PAT is not the source system. eRA is the source system. eRA maintains its own processes to obtain consent when major changes occur. eRA maintains its own PIA.

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.

PAT is not the source system. eRA is the source system. eRA maintains processes to resolve concerns an individual might have. eRA maintains its own PIA.

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

PAT is not the source system. eRA is the source system. eRA maintains processes for periodic reviews of data. eRA maintains its own PIA.

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.

When PII is collected, it is the minimal information needed in accordance with HHS and NIH Least Privilege policies. This means if staff (employees and direct contractors) have access to PII, it will be only minimally sensitive, the least PII needed, and will be used only in accordance with HHS and NIH security and privacy policies.

Administration staff is restricted to specific position within NIH. A 2- factor authentication will be used. All administrative staff will sign and comply with the system administrator rules of behavior to ensure HHS and NIH operational policies are followed regarding administrator privileges and technical-use for systems/applications.

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).

Users requesting remote access are required to take specialized training courses to include Securing Remote Computers and complete a Remote Access User Certification Agreement.

Users requesting Administrative rights to their assigned computers are required to complete the Federal Desktop Core Configuration (FDCC) Systems Administrator Training.

There are also role-based training requirements for staff designated as having "Significant IT Security Responsibilities." These include HHS role-based training courses for Executives, Managers, and IT Administrators.

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.

02-004, Extramural Program and Grants Management Oversight Records Cut off annually. Destroy 3 years after cutoff (DAA-0443-2013-0004).

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

Administrative Controls: PAT is classified as a Federal Information Security Modernization Act – Moderate system and goes through security assessment and authorization (SA&A) performed in accordance with NIH and HHS requirements. SA&A documentation including the following were

developed as required: security categorization, e-authentication risk assessment, system security plan, evidence of security control testing, and plan of action and milestones. Applicable Privacy Act clauses are inserted in solicitations and contracts as applicable. Policies for the retention and destruction of PII are in place. All personnel with access to the system are required to abide by the HHS and NIH Rules of Behavior and take a non-disclosure oath upon completing security awareness training as a new hire and then annually.

Technical Controls: User authentication (login) and logical access controls, anti-virus software, fire walls, role-based access through application. The database is behind a fire wall, with no direct access to it from outside the network.

Physical Controls: The server is housed in secure facility, climate control, fire alarm, fire extinguishers and Uninterrupted Power Supply (UPS).