US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/08/2024

OPDIV:

NIH

Name:

CIT BRICS Parkinson’s Disease Biomarker Program (PDBP)

PIA Unique Identifier:

P-3469942-025872

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?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Parkinson's Disease Biomarker Program (PDBP) is a collaborative cloud-based biomedical informatics system, created by the National Institute of Neurological Disorders and Strokes (NINDS), to accelerate the discovery of promising new diagnostic and progression biomarkers for Parkinson's Disease.

PDBP informatics system is a multi-faceted platform that makes it easier and faster for patients, caregivers and researchers to gather, evaluate, and share Parkinson's Disease research data from a variety of sources. The PDBP supports basic, translational and clinical research through hypothesis testing, target and pathway discovery, biomarker development, and disease modeling through broadly sharing data and biospecimens developed under this program.

Researchers with approved access to the Data Access Committee (DAC), PDBP have access to a number of tools, enabling them to share information and resources, which will accelerate the pace of

Parkinson's Disease biomarker discovery.

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

NIH collects and maintains the Principal Investigator's (PI's) name, email, university affiliation, publicly available videos and reports, username and password, mailing address, and phone numbers. The information is used by NIH to document, track, monitor and evaluate NIH clinical, basic, and population-based research activities, evaluate the use of PDBP datasets, and to notify recipients of updates, corrections, or other changes to PDBP.

The system collects and stores a wide variety of de-identified clinical information including medical history, vitals, brain scans, diagnostic data, genetics information, and data from diagnostic criteria specific to clinicians in the Parkinson's Disease field. All information, publicly available videos and reports, and data on research subjects (used to generate encrypted hashes that allow subject linking across studies for the same individuals) is maintained at the researcher's institution.

NIH staff requiring access to the system for administrative purposes 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 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.

PDBP informatics system is a multi-faceted platform that makes it easier and faster for patients, caregivers and researchers to gather, evaluate, and share Parkinson's Disease research data from a variety of sources. The PDBP supports basic, translational and clinical research through hypothesis testing, target and pathway discovery, biomarker development, and disease modeling through broadly sharing data and biospecimens developed under this program.

NIH collects and maintains the PI's name, email, university affiliation, publicly available videos and reports, username and password, mailing address, and phone number.

The information is used by NIH to document, track, monitor and evaluate the PI's clinical, basic, and population-based research activities, evaluate the use of PDBP datasets, and to notify recipients of updates, corrections, or other changes to PDBP.

The system collects and stores a wide variety of de-identified clinical information including medical history, vitals, brain scans, diagnostic data, genetics information, and data from diagnostic criteria specific to clinicians in the Parkinson's Disease field. All information, publicly available videos and reports, and data on research subjects (used to generate encrypted hashes that allow subject linking across studies for the same individuals) is maintained at the researcher's institution.

NIH staff requiring access to the system for administrative purposes log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

For additional and detail information about projects supported and policies can be found on the PDBP website at https://pdbp.ninds.nih.gov/

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
University affiliation, username and password
Publicly available videos and reports

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

Employees
Public Citizens

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

This information is used to document, track, monitor and evaluate clinical, basic, and population-based research activities, evaluate the use of PDBP datasets, and to notify recipients of updates.

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

N/A

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

42 U.S.C. 241, 42 U.S.C. 290dd-2, 42 CFR part 2, 5 U.S.C. 552a(m)

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.

09-25-0200 Clinical, Basic and Population-based Research Studies of the National Institutes of

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Within the DOC
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.

Users are notified as part of the application process.

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.

Access and submission is voluntary. If a PI doesn't want to provide the information, they won't have access.

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

Registered users of the system are notified via email of any major changes.

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.

PDBP users can notify the PDBP operations team for resolution. If there are additional concerns, they may 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 PDBP system policy requires yearly review of the accounts to ensure data/account integrity.

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 the PII is accessed, it is the minimal information needed in accordance with HHS and NIH Least Privilege policies. 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. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). 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 are required to complete Systems Administrator 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 01-001 - Records of Intramural Research Projects of Historical Significance
Intramural research records of relate to planning, development, oversight and execution of biomedical research projects and programs performed by NIH research staff, contractors or under collaborative research and development agreements (CRADAs).
Disposition: Cut off annually at termination of project/program or when no longer needed for scientific reference. Transfer to the National Archives in five year blocks when the newest records in the block are 15 years old. DAA-0443-2012-0007-0001

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

Administrative controls - Management oversight of activities, security awareness and training for users of the system, conduct disaster recovery exercises, separation of duties for personnel administering the system, isolating development test instances of the system. 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 require that each user log in to the PDBP application with a unique user name and password.

Physical controls - Server is housed in secure facility, climate control, fire alarm, fire extinguishers and Uninterrupted Power Supply (UPS) for servers. Badged access is required to all server rooms, with badge lockdown policies in line with existing NIH procedures. Physical server racks are key-locked.

Identify the publicly-available URL:

http://pdbp.ninds.nih.gov/

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?

Yes

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

Yes