US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/06/2026

OPDIV:

NIH

Name:

Biomedical and Biological Information System

PIA Unique Identifier:

P-4170425-190037

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

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.

Changed from Privacy Threshold Agreement (PTA) to a full Privacy Impact Assessment (PIA) to account for the data collection in the minor systems, under this major applications' system boundary.

Describe the purpose of the system.

The National Library of Medicine’s (NLM) Biomedical and Biological Information System (BBIS) is a collection of applications used for storing and analyzing data about molecular biology, biochemistry, and genetics.

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

The BBIS systems collect, maintain and share public molecular biology, biochemistry and genetics data.

BBIS systems collect name, email, phone number and mailing address and/or password. Users can submit information to databases as a Point of Contact (POC), create an account and/or get

information about laboratories offering tests and laboratory credentials.

Minor applications that make up the BBIS include:
Basic Local Alignment Search Tool (BLAST),
Clinical Trials,
Database of Genotypes and Phenotypes (dbGaP),
Genetic Testing Registry (GTR),
Sequence Read Archive (SRA),
GenBank,
PubChem,
PubMed and PubMed Central (PMC).

Each subsystem maintains its own unique privacy impact assessment (PIA) with all legal authorities documented and will list the BBIS Universally Unique Identifier (UUID) within their respective PIA. (GenBank, PubChem and PubMed are trademarked and are not acronyms).

Those requiring administrative access to BBIS 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 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 Service is an essential service which facilitates and governs network access to various resources.

For individuals external to NIH, such as business partners, collaborators, and researchers; the system uses NIH Federated Services, a centralized authentication hub for web-based applications at NIH, instead of storing a user's login credentials. NIH Federated login enables users to use a single authentication method via an individual's parent organization. After the system owner approves access to an individual and registers their parent organization's identity provider, individuals are redirected to their parent organization's identity provider for credentials. NIH Federation Services resides within the NIH IAM Services, and maintains its own PIA, including all legal authorities documented.

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

The BBIS collects, maintains and shares public molecular biology, biochemistry and genetics data. BBIS systems collect name, email, phone number, mailing address and/or password.

Users can submit information to databases as a POC, create an account and/or get information about laboratories offering tests and laboratory credentials.

Minor applications that make up the BBIS include:
BLAST - finds regions of similarity between biological sequences,
Clinical Trials - research studies that involve people and test new ways to prevent, detect, diagnose, or treat diseases.
dbGaP - an NIH repository charged to archive, curate and distribute information produced by studies investigating the interaction of genotype and phenotype.
GTR - provides a central location for voluntary submission of genetic test information by providers.
SRA - is the largest publicly available repository of high throughput sequencing data.
GenBank - is the NIH genetic sequence database, an annotated collection of all publicly available deoxyribonucleic acid (DNA) sequences.
PubChem - the world's largest collection of freely accessible chemical information.

PubMed - a free database including primarily the MEDLINE database of references and abstracts on life sciences and biomedical topics.
PMC - a free digital repository that archives open access full-text scholarly articles that have been published in biomedical and life sciences journals.

Each subsystem maintains its own unique PIAs with all legal authorities documented and will list the BBIS UUID within their respective PIA.

Those needing to administer the BBIS log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented. For individuals external to NIH, the system uses NIH Federated Services which resides within NIH IAM Services, and maintains its own PIA, including 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
Laboratory credentials (certification and licensure)
Username, password

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?

Personally identifiable information (PII) is provided in order to:
set up an account,
submit information to databases as a POC,
get information about laboratories offering tests.

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

There are no secondary uses for PII.

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

42 U.S.C. section 286, 42 U.S.C. § 282(i) and (j)), 44 U.S.C. Sec. 2904, 42 U.S.C. 241. 402(i) and 402(j) of the Public Health Service Act

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.

09-90-0777 - Facility and Resource Access Control Records

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

09-25-0200; Clinical, Basic and Population-based

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

0925-0651, Genetic Testing Registry, Under review.

0925-0670 ; NIH Information Collection Forms to Support Genomic Data Sharing for Research Purposes, Expiration Date: 04/30/2026

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.

None at this time.

Describe the procedures for accounting for disclosures.

Audit logs are used to disclose what information is shared.

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

PII is voluntarily submitted by individuals. A confirmation email is sent once an individual subscribes to verify that the individual wants to be signed to the email lists. Additionally, submitters are required to review and agree to a code of conduct statement before submitting PII information.

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.

Individuals may un-subscribe at any time through the website. Individuals may also reach out to the NLM help desk if they need further help. Submission users cannot opt-out of providing contact information, as it is necessary to have contact info for the data submitter.

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

Individual submitters are notified of changes to their personal and/or personally submitted PII data via email. Users may update or change the PII provided previously at any time. PII within the system is not changed or modified.

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.

PII is entered by the individual and may be edited at any time by the individual themselves.

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

Periodic data integrity audits are conducted by Administrative Staff.

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.

Individuals are verified through a confirmation email and only have access to their PII.

Periodic review of system users' roles is done to assure access is current with user's technical/functional role in administering, developing, and supporting the daily job functions.

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.

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.

10-101 - Administrative records maintained in any agency office.
Administrative records maintained in any agency office. Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists, excluding records scheduled elsewhere in the GRS such as timekeeping and procurement.
Disposition: Destroy when business use ceases. DAA-GRS2016-0016-0001

07-204 - System access records; Systems requiring special accountability for access.
These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.

Disposition: 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

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

Administrative Controls: System administrators are approved for access based on their technical/functional role in administering, developing, and supporting National Center for Biotechnology Information (NCBI) daily job functions, and administrators perform periodic reviews to assure users adhere to system policies.

Technical Controls: Access to the system is controlled by NIH IAM Services log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.

Physical Controls: The servers reside in the NLM Data Center where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and biometrics and badging requirements to the data center.

Note: web address is a hyperlink.