US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/27/2026

OPDIV:

NIH

Name:

Data COUNTS Trusted Data Broker Platform

PIA Unique Identifier:

P-8291518-700455

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Development

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.

Contractor

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.

Healthcare sites within the United States are required by law to share within the HHS and its Operational Divisions and Agencies for public health tracking and research purposes, which creates a significant burden for these sites. The Data Collect Once Use NumerouS Times (Data COUNTS) Initiative and system streamline and standardizes data collection from clinical sites by enabling data to be collected once and reused across HHS, reducing burden and minimizing errors through the Data COUNTS Trusted Data Broker (Data COUNTS TDB) system. The Foundation for the National Institutes of Health and its contractors, under NIH leadership, will serve as the Trusted Data Broker (TDB), transforming de-identified Electronic Health Records (EHR) data into a secure, usable format for research and agency mission work, with traceability and near real-time aggregation on Data COUNTS TDB. Clinical sites maintain control of their patients' data by choosing when to share data; eventually patients will have individual control over their data through establishing a Patient Trust Model (PTM). The Data COUNTS Initiative is targeting support of HHS use cases that provide federated data access for programs.

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

The system maintains the following personally identifiable information (PII): name, email, organizational affiliation, and usernames. These PII data elements are used to assign permissions and identify points of contact for partnered data sites and repositories.

The system maintains de-identified data of Electronic Health Records (EHR) coming directly from healthcare partners. These are non-identifiable limited data sets (LDS) which include time-shifted dates of service (such as admission, discharge), birth and death year, zip3, visits & procedure occurrences, diagnosis, diseases, prescription & drugs, medical devices and supplies, medical conditions, and health care provider locations.

Data COUNTS TDB employees and users log in using one of the following:

NIH Identity, Credential, and Access Management (IAM) Services, which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented.

In-Common, through NIH IAM Services, provides single sign-on (SSO) access to cloud and local services to hundreds of participating educational institutions, research organizations, and commercial resource providers.

HHS Personal Identity Verification (PIV), a US Federal government wide credential used to access Federally controlled facilities and information systems at the appropriate security level.

Login.gov, a publicly available secure online Government resource which allows a safe way to sign in to many U.S. government websites using just one account.

Data COUNTS TDB is hosted on the Palantir Foundry Cloud Service (PFCS) platform, a Federal Risk and Authorization Management Program (FedRAMP) authorized cloud service provider.

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

Healthcare sites within the United States are required by law to share within the HHS and its Operational Divisions and Agencies for public health tracking and research purposes, which creates a significant burden for these sites. The Data COUNTS Initiative and system streamline and standardizes data collection from clinical sites by enabling data to be collected once and reused across HHS, reducing burden and minimizing errors through the Data COUNTS TDB system. The Foundation for the National Institutes of Health and its contractors, under NIH leadership, will serve as the TDB, transforming de-identified Electronic Health Records (EHR) data into a secure, usable format for research and agency mission work, with traceability and near real-time aggregation on Data COUNTS TDB. Clinical sites maintain control of their patients' data by choosing when to share data; eventually patients will have individual control over their data through establishing a Patient Trust Model. The Cross-HSS Patient Health Data Initiative is targeting support of HHS use cases that provide federated data access for programs.

The system maintains the following personally identifiable information (PII): name, email, organizational affiliation, and usernames. These PII data elements are used to assign permissions and identify points of contact for partnered data sites and repositories.

The system maintains de-identified data of Electronic Health Records (EHR) coming directly from healthcare partners. These are non-identifiable limited data sets (LDS) which include time-shifted dates of service (such as admission, discharge), birth and death year, zip3, visits & procedure occurrences, diagnosis, diseases, prescription & drugs, medical devices and supplies, medical conditions, and health care provider locations.

Data COUNTS TDB employees and users log in using one of the following:

NIH Identity, Credential, and Access Management (IAM) Services, which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented.

In-Common, through NIH IAM Services, provides single sign-on (SSO) access to cloud and local services to hundreds of participating educational institutions, research organizations, and commercial resource providers.

HHS Personal Identity Verification (PIV), a US Federal government wide credential used to access Federally controlled facilities and information systems at the appropriate security level.

Login.gov, a publicly available secure online Government resource which allows a safe way to sign in to many U.S. government websites using just one account.

Data COUNTS TDB is hosted on the Palantir Foundry Cloud Service (PFCS) platform, a Federal Risk and Authorization Management Program (FedRAMP) authorized cloud service provider.

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
Organizational affiliation
Clinical Site Contributors
username

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

Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Clinical Site Contributors

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

Employee, Business Partner, and Contractor PII are required to manage, operate, and maintain the Data COUNTS TDB information technology platform, as well as perform quality assessments and research on the contributed data.

Clinical Site Contributors PII is required to grant contributing data sites access to submit , review and perform quality assessments on submitted data.

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

N/A. No secondary uses.

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

5 U.S. Code §301

42 U.S. Code § 281

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

09-25-0200, 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

In-Person

Government Sources

Within the OPDIV

Other HHS OPDIV

Non-Government Sources

Private Sector

Additionally, PII used to create an account solely for access is exempt from the requirements of the Paperwork Reduction Act.

Identify the OMB information collection approval number and expiration date

Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

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.

Prior notice is not required because researchers, business partners/collaborators voluntarily sign data agreements when requesting access to Data COUNTS TDB.

Employees and direct contractors voluntarily provide their personal information during the HHS staff onboarding 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.

There is no process for individuals to opt-out of providing their PII. Under the data transfer agreements, Clinical Site Contributors voluntarily provide their PII when requesting access to Data COUNTS TDB.

Employee PII are acquired based on their roles and responsibilities to develop, operate, and maintain the system. Thus, there is no opt-out option.

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

The process to notify and obtain consent is published in the Data COUNTS TDB website privacy notice. Changes to the policy will be posted on the Data COUNTS TDB website with a notable Notice alert to the changes.

For employees, Data COUNTS TBD is not the source system. Individuals are notified during the on-boarding process.

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 reach out to Data COUNTS TDB Platform support by submitting a help desk ticket, under the General Support category.

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

Site Contributor PII reviews are conducted following standard on-boarding and off-boarding processes, during annual renew account reviews, and/or the termination of the DTUA.

For employee data, Data COUNTS TDB is not the source system. Source systems that maintain employee PII have their own processes for periodic reviews of PII within the system.

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. The system uses NIH IAM services/ Login.gov/ PFCS Role Based Access Control (RBAC)/ PFCS Attributed-Based Access Control (ABAC) services to assign permissions/user roles which is considered PII.

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.

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.

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 or https://irtsectraining.nih.gov/publicuser site for users/contractors without NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

Users are provided links to Palantir training material on data protection tools, understanding projects and roles, processes for requesting access to specific data views or subsets, and government and industry standards and compliance considerations.

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 03-005 - Patient Medical Records. Cut off patient case file annually after 5 years of inactivity. Destroy when case file is no longer needed for scientific reference (DAA-0443-2012-0007-0010).

01-003, Records of All Other Intramural Research Projects. Cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer. 7 years after cutoff (DAA-0443-2012-0007-0003).

08-205, Information access and protection operational records. Access control records. Destroy when superseded or obsolete, but longer retention is authorized if required for business use (DAA-GRS-2013-0007-0020).

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

Administrative
Users log in using secure government authentication and authorization systems based on assigned permissions. Permissions are determined by the Data COUNTS TDB Account Management Team. Administrative controls are reinforced by the technical and physical controls laid out below.

Technical
Data COUNTS TDB is hosted on Palantir Foundry Cloud Service (PFCS), a FedRAMP authorized cloud service. Technical security controls are documented in the Data COUNTS TDB System Security Plan and leveraged FedRAMP Authorization packages and contractor's management service of the platform ensures that data is secured in the system via several technical means. Across the platform, data is encrypted in transit and at rest. PFCS provides highly configurable access controls. The PFCS platform supports comprehensive auditing of all data processing and access. It captures meta-data about the source of all data and maintains records of data imports, reads, writes, searches, exports, and deletions.

Physical
PFCS is a cloud service platform hosted in Amazon Web Services (AWS). The PFCS system architecture is aligned with industry standard frameworks and maintains a FedRAMP Authorization with a security categorization of High, which allows it to store and process sensitive data.

Identify the publicly-available URL:

https://dcounts-tdb.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