US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/27/2026

OPDIV:

NIH

Name:

Information Management Services Application Support Environment

PIA Unique Identifier:

P-6916908-975185

The subject of this PIA is which of the following?

General Support System (GSS)

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.

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.

The Information Management Services Application Support Environment (IMS ASE) computer center is a General Support System providing resources for microcomputer and client/server applications development and hosting, Linux server analytic software, Structured Query Language (SQL) server applications development, electronic mail, web application development, and website hosting.

The IMS ASE maintains sub-systems, data repositories, and controlled access data repositories (CADRs) in its function as a trusted data broker, collecting and managing clinical and research data of the Center for Disease Control (CDC) National Breast and Cervical Cancer Early Detection Program (NBCCEDP) and Colorectal Cancer Control Program (CRCCP), National Institute of Aging (NIA), National Institute of Mental Health (NIMH), National Institute on Minority Health and Health Disparities (NIMHD), National Cancer Institute (NCI), State Cancer Repositories, and study partners of the institutes and centers within NIH and CDC listed above.

IMS ASE’s two CADRs are:

Cancer Data Access System (CDAS): A web-based system for requesting access to data, biospecimens, and images from cancer screening trials and other studies, facilitating review of requests, delivering data, and publishing approved projects and related publications for public use.
Medicare Health Outcomes Survey (MHOS): A dataset used to research health outcomes in cancer. Providing information about the health-related quality of life (HRQOL) of Medicare Advantage Organization enrollees.

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

The IMS ASE maintains the following personally identifiable information within its subsystems, data repositories, and CADRs for the purpose of supporting cancer research across the nation to advance scientific knowledge.

Name, email, Social Security Number (SSN), driver's license number, mother's maiden name, phone number, biometric identifiers, medical notes, certificates, education records, military status, foreign activities, taxpayer ID, date of Birth (DoB), photographic identifiers, mailing address, medical records numbers (MRNs), genomic data, device identifiers, employment status, login credentials (usernames, passwords).

IMS ASE and its subsystems and repositories use specific login information to assign permissions/user roles which are considered Personally Identifiable Information (PII).

However, this is done by using the following access tools and processes:

This login information is stored within an MS Active Directory (AD) service that is used for authorizing computers, users, and applications for use within the IMS ASE. The AD service governs network access to all resources inside the IMS ASE.

For limited web application access controls, IMS ASE incorporates NIH Login, a module of the NIH Identity, Credential, and Access Management (IAM) Services. IAM maintains its own Privacy Impact Assessment.

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

Federated login, a centralized authentication for web-based applications. Instead of storing a user's login credentials, federated login enables users to use a single authentication method via an individual's parent organization.

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

The Information Management Services Application Support Environment (IMS ASE) computer center is a General Support System providing resources for microcomputer and client/server applications development and hosting, Linux server analytic software, Structured Query Language (SQL) server applications development, electronic mail, web application development, and website hosting.

The IMS ASE maintains sub-systems, data repositories, and controlled access data repositories (CADRs) in its function as a trusted data broker, collecting and managing clinical and research data of the Center for Disease Control (CDC) National Breast and Cervical Cancer Early Detection Program (NBCCEDP) and Colorectal Cancer Control Program (CRCCP), National Institute of Aging (NIA), National Institute of Mental Health (NIMH), National Institute on Minority Health and Health Disparities (NIMHD), National Cancer Institute (NCI), State Cancer Repositories, and study partners

of the institutes and centers within NIH and CDC listed above.

IMS ASE's two CADRs are:

Cancer Data Access System (CDAS): A web-based system for requesting access to data, biospecimens, and images from cancer screening trials and other studies, facilitating review of requests, delivering data, and publishing approved projects and related publications for public use. Medicare Health Outcomes Survey (MHOS): A dataset used to research health outcomes in cancer. Providing information about the health-related quality of life (HRQOL) of Medicare Advantage Organization enrollees.

The IMS ASE maintains the following personally identifiable information within its subsystems, data repositories, and CADRs for the purpose of supporting cancer research across the nation to advance scientific knowledge.

Name, email, Social Security Number (SSN), driver's license number, mother's maiden name, phone number, biometric identifiers, medical notes, certificates, education records, military status, foreign activities, taxpayer ID, date of Birth (DoB), photographic identifiers, mailing address, medical records numbers (MRNs), genomic data, device identifiers, employment status, login credentials (usernames, passwords).

IMS ASE and its subsystems and repositories use specific login information to assign permissions/user roles which are considered Personally Identifiable Information (PII).

However, this is done by using the following access tools and processes:

This login information is stored within an MS Active Directory (AD) service that is used for authorizing computers, users, and applications for use within the IMS ASE. The AD service governs network access to all resources inside the IMS ASE.

For limited web application access controls, IMS ASE incorporates NIH Login, a module of the NIH Identity, Credential, and Access Management (IAM) Services. IAM maintains its own Privacy Impact Assessment.

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

Federated login, a centralized authentication for web-based applications. Instead of storing a user's login credentials, federated login enables users to use a single authentication method via an individual's parent organization.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
Biometric Identifiers
Mother's Maiden Name
E-Mail Address
Mailing Address

Phone Numbers
Medical Records Number
Medical Notes
Certificates
Education Records
Device Identifiers
Military Status
Employment Status
Foreign Activities
Taxpayer ID
User Credentials, Genomic Data

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

Employees
Public Citizens
Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The primary purpose of the collected PII is to support a broad range of research, training, and information dissemination activities across the entire country and with research partners.

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

PII is used secondarily to assign permissions within the site. Limiting PII access to vetted and approved users.

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

Public Health Service Act. (42 U.S.C. 241, 242, 248, 281, 282, 284, 285a-285q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101)

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
Online
Government Sources
Within the OPDIV
Other HHS Operating Divisions
Non-Governmental Sources
Public

Identify the OMB information collection approval number and expiration date

Not Applicable. The collection of PII to create an account solely for access is exempt from the requirements of the Paperwork Reduction Act or Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

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.

Individuals that have access to PII within the IMS ASE subsystems, repositories, and CADRs must sign data use agreements (DUAs) after submitting their application forms for review and approval.

Describe the procedures for accounting for disclosures.

IMS ASE subsystems, repositories, and CADRs account for disclosures by limiting data access to approved users. DUAs are kept and outline which datasets users have access to PII in.

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

IMS ASE and its subsystems, repositories, and CADRs are not the sources of PII collection. These partnered systems, including state cancer repositories, maintain their own processes to notify individuals that their PII is being collected.

For PII that is used for access control and permissions, users are notified when they fill out their applications for access to the system.

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.

IMS ASE is not the source system. Opt-out methods are handled at the time of PII collection. This includes by Principal Investigators (PIs), state cancer registries, and clinical research partners.

For PII used for access and permissions, there is no opt-out option. Users may decide to not provide their PII during the application process, but that would result in individuals not being granted access to IMS ASE and its subsystems, repositories, and CADRs.

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

IMS ASE is not the source system. Processes to notify and obtain consent when major changes occur are handled at the time of PII collection. This includes by Principal Investigators (PIs), state cancer registries, and clinical research partners.

For PII used for access and permissions, there is no opt-out option. Users are notified by email and webpage notifications when major changes occur.

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.

There is a “Contact Us” page on the IMS ASE webpages that users use to submit concerns about how PII has been obtain, used, or disclosed, or if it is inaccurate. Upon submitting the concern, a

member of the IMS ASE Help Desk responds to the reporting individual by their preferred method of communication.

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

IMS ASE is not the source system. Periodic reviews are handled at the time of PII collection. This includes by Principal Investigators (PIs), state cancer registries, and clinical research partners.

For PII used for access and permissions, user accounts are periodically reviewed by IMS ASE administrators to ensure compliance with all IMS ASE policies and procedures.

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.

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.

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

Users of the IMS ASE are required to participate in role-based training for their job functions. This includes human subject research training for individuals that may work with human subject research data.

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.

07-203, System access records. Systems not requiring special accountability for access. Destroy when business use ceases (DAA-GRS-2013-0006-0003).

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. Destroy 7 years after cutoff (DAA-0443-2012-0007-0003).

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

Administrative Controls: Access level and permissions are controlled by the system and based on approval by NCI during NCI's review of the data access requests.

Technical Controls: Access to the system is controlled by login authentication of users prior to granting access. 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 data is stored within the Information Management Services Application Support Environment, a Federal Information Security Modernization Act (FISMA) of 2014 moderate audited system which is hosted in co-location facilities in Sterling, VA and Baltimore, MD. The facilities provide secure infrastructure and restricted physical access to servers and administrative systems, ensuring that only authorized personnel can manage or maintain the environment.

Identify the publicly-available URL:

https://aghealth.nih.gov
https://agingresearchbiobank.nia.nih.gov
https://api.seer.cancer.gov
https://applications.prevention.cancer.gov
https://atbcstudy.cancer.gov
https://biolincc.nhlbi.nih.gov
https://cdas.cancer.gov
https://cdp.nci.nih.gov
https://chtn.cancer.gov
https://cisnet.cancer.gov
https://cpfp.cancer.gov
https://crccp.cdc.gov
https://ctrandomization.cancer.gov
https://dceg2.cancer.gov
https://dcptools.cancer.gov
https://emblem.cancer.gov
https://epi.grants.cancer.gov
https://gis.cancer.gov
https://hdpulse.nimhd.nih.gov
https://healthcaredelivery.cancer.gov
https://knowyourchances.cancer.gov
https://lfs.cancer.gov
https://marrowfailure.cancer.gov
https://metabolomics-sig.nih.gov
https://mydcp.cancer.gov
https://nbccedp.cdc.gov
https://nccrexplorer.ccdi.cancer.gov
https://ncorp.cancer.gov
https://nctnbanks.cancer.gov
https://neurobiobank.nih.gov
https://portals.dceg.cancer.gov
https://ppb.cancer.gov
https://prevention.cancer.gov

https://progressreport.cancer.gov
https://radi
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