US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/05/2025

OPDIV:

NIH

Name:

NIH Qlik Sense Cloud - Intramural

PIA Unique Identifier:

P-6530817-764236

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?

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 NIH Qlik Sense Cloud - Intramural is a data analytics platform allowing NIH users the ability to combine and load data for fast-track reporting analysis. Qlik Sense Cloud transforms data into visually appealing, interactive visualizations and dashboards.

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

Information held within NIH Qlik Sense Cloud - Extramural comes from source systems at NIH that maintain their own Privacy Impact Assessments (PIA), including all legal authorities documented. While Personally Identifiable Information (PII), and sensitive information will be held within the system, the end user dashboards and analytics will be aggregated and de-identified.

The type of data and information that NIH Qlik Sense Cloud - Intramural will collect, maintain, and/or share includes: Name, Mother's maiden name, email, phone numbers, medical notes, date of birth, mailing address, medical record numbers, device identifiers, employment status, and Photographic and Biometric Identifiers.

Users log in to this system using the NIH Identity, Credential, and Access Management (ICAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of ICAM 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 ICAM Services collect unique user credentials and stores them in an encrypted format. The ICAM 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 NIH Qlik Sense Cloud - Intramural is a data analytics platform allowing NIH users the ability to combine and load data for fast-track reporting analysis. Qlik Sense Cloud transforms data into visually appealing, interactive visualizations and dashboards.

Information held within NIH Qlik Sense Cloud - Extramural comes from source systems at NIH that maintain their own Privacy Impact Assessments (PIA), including all legal authorities documented. While Personally Identifiable Information (PII), and sensitive information will be held within the system, the end user dashboards and analytics will be aggregated and de-identified.

The type of data and information that NIH Qlik Sense Cloud - Intramural will collect, maintain, and/or share includes: Name, Mother's maiden name, email, phone numbers, medical notes, date of birth, mailing address, medical record numbers, device identifiers, employment status, and Photographic and Biometric Identifiers.

Users log in to this system using the NIH Identity, Credential, and Access Management (ICAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of ICAM 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 ICAM Services collect unique user credentials and stores them in an encrypted format. The ICAM 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.

Date of Birth
Photographic Identifiers
Biometric Identifiers
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Device Identifiers
Employment Status

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?

10,000-49,999

For what primary purpose is the PII used?

The primary purpose that the PII will be used is to create summarized and aggregated information to populate dashboards for statistical analysis of trends and trend forecasting for NIH.

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

NA

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, 282, 284, 285a-j, 285 l-q, 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.

09-25-0099; Clinical Research: Patient Medical Records, HHS/NIH/CC

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

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A. This system is exempt from an OMB Information Collection Number through Public Law 114-255 - 21st Century Cures Act, Section 2035: Exemption for the National Institutes of Health from the Paperwork Reduction Act 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.

NIH Qlik Sense Cloud - Intramural is not a source system. PII is not collected directly from individuals. Source system operators are responsible for notifying individuals about the uses of their personal information and is covered in the respective source system 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.

NIH Qlik Sense Cloud - Intramural is not a source system. Personal information is not collected directly from individuals. Source system operators are responsible for providing a method to opt-out of the collection and use of their PII.

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

NIH Qlik Sense Cloud - Intramural is not a source system. Personal information is not collected directly from individuals. Source system operators are responsible for providing a process to notify and obtain consent from individuals whose PII is in the system 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.

NIH Qlik Sense Cloud - Intramural is not a source system. Personal information is not collected directly from individuals. Source system operators are responsible for putting a process in place to resolve an individual's concerns about the collection and use their PII. However, individuals may contact any IC Privacy office, or the NIH Senior Official for Privacy.

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

NIH Qlik Sense Cloud - Intramural is not a source system and does not have process in place to review PII. Personal information is not collected directly from individuals. Source system operators are responsible periodically reviewing PII contained in the source systems to ensure data integrity, availability, accuracy, and relevance.

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).

Additionally, the NIH Analytics Community of Practice (NACoP) provides recorded training/demonstrations to Qlik Sense Cloud users.

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.

03-001, Clinical Care Services Records, DAA-0443-2019-0001-0001, and are temporary records that can be destroyed seven years after cutoff.

03-005, Patient Medical Records, DAA-0443-2012-0007-0010, are temporary records that can be destroyed after five years of inactivity or when no longer needed for scientific reference.

03-002, Radiology and imaging Records, DAA-0443-2012-0007-0007, are temporary records that can be destroyed 60 years after inactivity.

03-003, Blood Donor and Receiving Records, DAA-0443-2012-0007-0008, are temporary records that shall be retained for such intervals beyond the expiration date for the blood or blood component as necessary to facilitate the reporting of any unfavorable clinical reactions as required by 21 CFR 606. The records may be destroyed 30 years after cutoff, which is 50 years or annually after expiration of the patient/subject, whichever is longer.

03-006, Medical Staff Credentialing Records, DAA-0443-2012-0007-0011, are temporary records that can be destroyed 30 years after cutoff, which is one year after the medical staff member leaves patient care.

03-007, Pathology Test Records, DAA-0443-2012-0007-0012, are temporary records that can be destroyed 10 years after cutoff, which is one year after the date of reporting.

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.

Technical controls - User authentication (login) and logical access controls (IAM, PIV card, and network access), 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. Data loss prevention software is enabled, as well as multi-factor authentication.

Physical controls - Server housed in secure facility, climate control, fire alarm, fire extinguishers and Uninterrupted Power Supply (UPS) for servers.