US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/20/2025

OPDIV:

CMS

Name:

Informatica BI

PIA Unique Identifier:

P-8142640-973680

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.

Annual Review and Recertification

Describe the purpose of the system.

Informatica is an Extract, Transform, and Load tool used for transferring or transporting information from one Centers for Medicare and Medicaid Services information system to another Centers for Medicare and Medicaid Services information system. It is an internal application within the Centers for Medicare and Medicaid Services and not connected to any external system or website. Using Informatica allows the Centers for Medicare and Medicaid Services to conduct a broad range of internal business functions.The primary function of the Extract, Transform, and Load tool is to ensure data is loaded in the desired target systems. The sources and targets vary based on the business needs. The target systems are then used for running queries or generating any reports using reporting tools by end users. The Application teams should be contacted for any specifics about the business functions. Our group provides the framework and support of the Informatica infrastructure

only.

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

The only information that Informatica maintains is system user credentials, user identification, password, and job code. User access is validated by the Enterprise User Administration system.The information that Informatica extracts, transforms, and loads between systems depends on the source system. The information may include name, address, telephone number, date of birth, Social Security Number, a Health Insurance Claim Number, medical notes, medical records number, Unique Provider Identifier Number, sex, and race/ethnicity.The systems mentioned here have their own Privacy Impact Assessment and Authority to Operate.

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

Informatica is an internal to the Centers for Medicare and Medicaid Services application tool that provides the mechanism for data to be integrated, accessed, and shared between the Centers for Medicare and Medicaid Services information systems through the Extract, Transform, and Load process. Using the Informatica tool encourages collaboration between the Centers for Medicare and Medicaid Services business components and allows the Centers for Medicare and Medicaid Services systems to maintain, share, and reuse data for projects.The information/data that is shared among systems is maintained and stored within those Centers for Medicare and Medicaid Services systems and may include Personable Indentifiable Information. As such, each Centers for Medicare and Medicaid Services source system is responsible for maintaining the security of the Personable Indentifiable Informationand corresponding Privacy Impact Assessment. These source systems are:

- Durable Medical Equipment, Prosthetics, Orthotics, & Supplies Bidding System
- Reusable Framework Application
- Integrated Data RepositoryInformatica uses the Enterprise User Administration system for system user identification and authentication. User credential information is maintained at user logon and is passed to the Enterprise User Administration for verification and validation before the user is able to log into the system. Informatica will validate the job codes and based on the codes in the Enterprise User Administration, will grant user access to view system-specific information. System users are either Centers for Medicare and Medicaid Services employees or direct contractors. The only information that Informatica collects on users is system user credentials, user identifcation, password, and job code.The systems mentioned here have their own Privacy Impact Assessment and Authority to Operate.

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
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Other: User ID, password, Job code, HICN, UPIN, Race, Sex

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

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Informatica provides Extract, Transform, and Load functions for other Centers for Medicare and Medicaid Services systems and only transports Personal Identifiable Information elements because of the other system's data feeds. Informatica allows the systems to perform their business function/mission by performing these Extract, Transform, and Load functions on their behalf. User credentials are utilized for user authentication and access.When the Extract, Transform, and Load job runs, it pulls the data from the source system on to the Informatica server in the form of data cache files. Once all the transformations are applied based on the mapping rules, the data is then pushed to the target system and the caches are released. In the case of flat files, where files need to be created as part of the business need, the files will reside on the Application specific folders until they are archived. The access is restricted to the Application teams who owns these files.The systems mentioned here have their own Privacy Impact Assessment and Authority to Operate.

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

Not applicable.

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

Sections 226, 226A, 1811, 1818, 1818A, 1831, 1833(a)(1)(A), 1836, 1837, 1838, 1843, 1866, 1874a, 1875, 1876, 1881, and 1902(a)(6) of the Social Security Act.Title 42 of the United States Code: 426, 426–1, 1395c, 1395i–2, 1395i–2a, 1395j, 1395l(a)(1)(A), 1395o, 1395p, 1395q, 1395v, 1395cc, 1395kk–l, 1395ll, 1395mm, 1395rr, 1396a(a)(6), and § 101 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (Pub. L. 108–173).Section 10332 of the Affordable Care Act.5 United States Code Section 301, Departmental Regulations.

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable.

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.

The Informatica system only maintains the Enterprise User Administration user credentials. Notification that personal information is maintained occurs at the system log-in, where the Centers for Medicare and Medicaid Services warning banner is presented to the system user. All other Personable Identifiable Information that may be processed by the system is maintained by the following the Centers for Medicare and Medicaid Services source systems, which are each covered by their own Privacy Impact Assessment: Durable Medical Equipment, Prosthetics, Orthotics, & Supplies Bidding System• Reusable Framework Application, Integrated Data Repository. It is the responsibility of each source system to notify individuals that their Personal Identifiable Information

will be collected. The systems mentioned here have their own Privacy Impact Assessment and Authority to Operate.

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.

To access the system, a user must input their user credentials Personal Identifiable Information. Therefore, there is no option to opt-out. All other Personal Identifiable Information that may be processed by the system is maintained by the following the Centers for Medicare and Medicaid Services source systems, which are each covered by their own Privacy Impact Assessment:

• Durable Medical Equipment, Prosthetics, Orthotics, & Supplies Bidding System, Reusable Framework Application, Integrated Data Repository. It is the responsibility of the source system to notify individuals of how to opt-out of the collection or use of their Personal Identifiable Information. The systems mentioned here have their own Privacy Impact Assessment and Authority to Operate.

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

If there were any major changes to the system that affected system users, they would be notified by the Centers for Medicare and Medicaid Services via email as part of their normal End User Notification. The Centers for Medicare and Medicaid Services employees or direct contractors give overall consent to the collection of Personal Identifiable Information and use of government systems as part of the employment or access to systems process. All other Personal Identifiable Information that may be processed by the system is collected by the following Centers for Medicare and Medicaid Services source systems, which are each covered by their own Privacy Impact Assessment: Durable Medical Equipment, Prosthetics, Orthotics, & Supplies Bidding System• Reusable Framework Application, Integrated Data Repository. It is the responsibility of the source system to notify and obtain consent from the individuals whose Personal Identifiable Information is in the system when major changes occur to the system. The systems mentioned here have their own Privacy Impact Assessment and Authority to Operate.

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.

An individual’s concerns will be considered, investigated, and resolved in the following manner: If a system user has concerns about their Personal Identifiable Information, they would contact the Centers for Medicare and Medicaid Services Information Technology Service Help Desk and report any issues by email or telephone. The Help Desk would investigate and determine if any action needs to be taken by either the user or the Information Technology department.

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

Informatica maintains the data integrity and availability by employing security procedures including firewalls, requiring complex passwords, role based access and encryption layers. The users of the system and Informatica administrators maintain data accuracy and relevancy. Users can correct their own Personal Identifiable Information data within their own Enterprise User Administration account, or administrators can correct this for them if they are alerted to changes. Administrators also run quarterly reports to determine if there are any anomalies (i.e. name change, or mismatch) with user information. If found, the error is addressed and resolved by contacting the user, and modifying their user data, or by removing their access to Informatica, if no longer required.The systems mentioned here have their own Privacy Impact Assessment and Authority to Operate.

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 Personal Identifiable Information is managed by the Enterprise User Administration job code assigned to each user. The job codes dictate the permissions to access Personal Identifiable Information based on the principle of 'least privilege'.

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.

Each Informatica server is associated with a separate Enterprise User Administration job code and only users with approved Enterprise User Administration job codes are granted access to the specified Extract, Transform, and Load server. Each project on the Extract, Transform, and Load server is owned by a separate UNIX application account and group and only users with approved project jobcodes are granted access to the appropriate project folders.The systems mentioned here have their own Privacy Impact Assessment and Authority to Operate.

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.

The Centers for Medicare and Medicaid Services employees and direct contractors, who access The systems, are required to take the annual Security and Privacy Awareness Training and recertify the training each year. At the end of the training course, a test is taken to verify the completion of the training.

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

System users and developers are required to complete Role Based Security Training based on their position. Depending on the role, they are required to take a different number of hours of additional security training per year.

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.

Informatica follows the Centers for Medicare and Medicaid Services Records Schedule published in the National Archives and Records Administration General Records Schedule Disposition Authority Agency - General Records Schedules-2013-0006-0003 is used stating to "Destroy 1 year(s) after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is appropriate."

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

The administrative controls are: the Enterprise User Administration is leveraged for user authentication and authorization services and conducts annual recertification of user access and privileges; access is disabled when no longer needed; and users are deactivated after 60 days of inactivity. There is also training required for use of the system. Technical protection is achieved through firewalls and intrusion detection systems; continuous monitoring for system usage and unexpected or malicious activity; the configuration of specialty hardware and the use of encryption, including full disk encryption of laptops and workstations.The system’s physical security controls consist of restricted access and environmental protections. Which consist of protected cooling and power sources. Access to this area is recorded, and restricted only to authorized personnel with

appropriate security clearance. Facility access is controlled using badge access card readers. Media destruction and disposal procedures are carried out by the Centers for Medicare and Medicaid Services Amazon Web Services.The systems mentioned here have their own Privacy Impact Assessment and Authority to Operate.