US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/17/2016

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.
No changes occurred.

Describe the purpose of the system.
Informatica is an Extract, Transform and Load (ETL) tool used for transferring or transporting information from one CMS information system to another CMS information system. It is an internal application within CMS and not connected to any external system or
Website. Using Informatica allows CMS to conduct a broad range of internal business functions.

Describe the type of information the system will collect, maintain (store), or share.
The only information that Informatica collects is system user credentials, user ID, password and job code.

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 (SSN), a Health Insurance Claim Number (HICN), medical notes, medical records number, Unique Provider Identifier Number (UPIN), gender, and race/ethnicity.

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 CMS application tool that provides the mechanism for data to
be integrated, accessed and shared between CMS information systems through the ETL process. Using the Informatica tool encourages collaboration between the CMS business components and allows CMS systems
to maintain, share, and reuse data for projects.

The information/data that is shared among systems is collected and stored within those CMS systems and may include PII. As such, each CMS system is responsible for maintaining the security of the PII and corresponding PIA.

Informatica uses the Enterprise User Administration (EUA) system for system user identification and authentication. User credential information is collected at user logon and is passed to EUA 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 EUA will grant user access to view system-specific information. System users are either CMS employees or direct contractors.

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, Gender

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

Employees

Public Citizens

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Informatica provides ETL functions for other CMS systems and only transports PII elements because of the other system's data
feeds. Informatica allows the systems to perform their business function/mission by performing these ETL functions on their behalf.

User credentials are utilized for user authentication and access.

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

Not applicable.

Describe the function of the SSN.

Informatica does not use SSNs directly. SSNs may be part of the data that is processed through Informatica. Use of the SSN depends on the needs of the consumer system and Informatica does not participate in the function of the SSN.

Cite the legal authority to use the SSN.

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 (the Act).

Title 42 of the United States Code (U.S.C.): 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 (MMA) (Pub. L. 108– 173).

Section 10332 of the Patient Protection and Affordable Care Act (ACA).

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 (the Act).

Title 42 of the United States Code (U.S.C.): 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 (MMA) (Pub. L. 108– 173).

Section 10332 of the ACA.

5 U.S.C. 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.

Informatica only collects user credentials. Notification that personal information is collected occurs at system log on, where there is the CMS warning banner is presented to the system user.

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 method for a system user to opt-out of providing PII, their user credentials, because it is required for system access.

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 the system users, they would be notified by CMS as part of the normal channels of information. CMS employees or direct contractors give overall consent to the collection of PII and use of government systems as part of the employment or access to systems 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.

If a system user has concerns about their PII, they would contact the CMS IT 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 IT 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 PII data within their own EUA 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.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Users may access PII during the ETL process of extracting and transferring data.

Administrators:

Administrators may access PII in order to manage user accounts.

Developers:

Developers are the users of the system and may access PII as part of the ETL process of data extraction and transfer.

Contractors:

Direct contractors, in their roles as user, administrator or developer, may have access to PII as described in those role explanations.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Access to PII is managed by the EUA job code assigned to each user. The job codes dictate the permissions to access PII 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 EUA job code and only users with approved EUA job codes are granted access to the specified ETL server. Each project on the ETL server is owned by a separate UNIX application account and group and only users with approved project job codes are granted access to the appropriate project folders.

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.

CMS employees and direct contractors, who access CMS 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.

The NARA General Records Schedule DAA-GRS-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 EUA 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.