US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/17/2017

OPDIV:

CMS

Name:

Cognos BI

PIA Unique Identifier:

P-6000700-306793

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 significant changes have occurred in the system.

Describe the purpose of the system.

Cognos is a Business Intelligence (BI) application that provides the Centers for Medicate and Medicaid Services (CMS) with a wide range of Business Intelligence (BI) functionality on a single Web services-based architecture. Cognos offers a complete range of BI functionality, including reporting, analysis, dash boarding, score carding and event management. Also, the system delivers a single metadata layer and a single query engine, providing CMS with a single source reporting tool for all relevant data and a complete and consistent view of any business issue or driver.

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

Cognos Business Intelligence (BI) software is used to report on customer data. Cognos BI acts only as a conduit (e.g., pass through) between the CMS-maintained data stores and the verticals.

Cognos utilizes CMS's Enterprise User Administration (EUA) and Enterprise Identity Management System (EIDM), which are covered by separate PIAs, for system user identification and authentication. Those systems are responsible for storing and maintaining user's credentials. Cognos stores user's credentials and validates user's against the required job codes in order to grant the user access to vertical-specific information during their active session.

The only information Cognos store is user IDs to verify user's job codes during their session. The information that is pass through between the CMS- maintained data stores and the verticals may include:

SSN, Medical Notes, Date of Birth, Mailing Address, Name, Phone Numbers, Medical Records, Health Insurance Claim Number (HICN), Unique Physician Identification Number (UPIN), Race, Sex, Diagnosis Codes, and Procedure codes.

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

Cognos Business Intelligence (BI) tool provides authorized CMS users with a single point of access to application and data resources. Business Intelligence enables access and analysis of information to improve and optimize decisions and performance. It offers a web-based window into applications or information that a user is authorized to access, without regard to their network connection based on their security access role to the data.

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.

Cognos stores user's credentials and validates user's against the required job codes in order to grant the user access to vertical-specific information during their active session. Cognos uses the Enterprise User Administration (EUA) and Enterprise Identity Management System (EIDM) 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. Cognos will validate the job codes and based on the codes in EUA will grant user access.

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

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?

Cognos provides BI functionality, including reporting, analysis, dashboards, scorecards, and event management. Cognos uses PII in a pass through method when providing these functionalities between the CMS-maintained data stores and the verticals. User credential PII is used to authenticate users of Congnos.

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

Not applicable.

Describe the function of the SSN.

Cognos does not use SSNs directly. When reporting on beneficiary records, the SSN is present to support appeal adjudication needs; but is not the key field/data element used.

Cite the legal authority to use the SSN.

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.

The CMS-maintained data stores leverage Section 10332 of the Patient Protection and Affordable Care Act (ACA).

The legal authority used to govern use of user's credentials is 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

Government Sources

Within OpDiv

Non-Governmental Sources

Public

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.

Notification that personal information is collected occurs at system logon, where there is a CMS warning banner presented to the system users.

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 the 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.

The data that Cognos passes from one system to another is not owned or housed by Cognos. Any concerns an individual may have with the data would be handled by the data's system owner. System users can correct their own PII data within their own EUA account.

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

Cognos does not store any PII data. It acts as a pass through of the data.

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

Users:

Users are given developer privileges as they are using Cognos to develop reports. Cognos provides mechanisms for them to retrieve data from another system.

Administrators:

Administrators may access PII in order to manager user accounts.

Developers:

Developers may access PII in order to perform system updates.

Contractors:

Direct contractors, in their roles as an 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 controls are put in place based on job codes and privileges which are approved by the system government task lead.

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.

Users of the system are provided access, using RBAC, to access only those data elements that their own system has access to and no more.

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.

Access to Cognos is done through EUA. CMS requires all EUA users to go through annual Security training and to recertify their account's job codes.

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

Not applicable.

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.

Cognos follows the CMS Records Schedule published in The National Archives and Records Association (NARA) General Records Schedule DAA-GRS-2013-0006-0005 is used stating to "Destroy when superseded by a full backup, or when no longer needed for system restoration, which ever is later."

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 consists of protected cooling and power sources. Access to this area is recorded, and restricted only to authorized personnel and appropriate security clearance. Facility access is controlled using badge access card reader.