US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/17/2017

OPDIV:

CMS

Name:

Arc Geographic Information System

PIA Unique Identifier:

P-7514704-275516

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?

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 purpose of the Arc Geographical Information System (ArcGIS) is to provide CMS with an enterprise solution that will enable geographic mapping and analysis to the Center for Program Integrity (CPI) to help meet its business objective of finding and reducing waste, fraud and abuse in Medicaid and Medicare. The ArcGIS tool will use data from the Integrated Data Repository (IDR), and will enhance it beyond longitude and latitude points currently stored at the ZIP code level to also include coordinates at the street-address level.

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

ArcGIS collects system user credentials - user ID, password and job code. System users are either CMS employees or direct contractors.

The information that ArcGIS extracts, transforms and loads (ETL) between CMS' IDR system depends on the source system.

The information may include name, address, telephone number,Social Security number (SSN), date of birth, a Health Insurance Claim Number (HICN), medical notes, medical records number, Unique Provider Identifier Number (UPIN), National Provider Identifier (NPI), 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.

ArcGIS will be used to extract, geocode, visualize, and analyze data to solve business problems such as detection of fraud, waste, and abuse. The ArcGIS tool will use data from the Integrated Data Repository (IDR), and will enhance it beyond longitude and latitude points currently stored at the ZIP code level to also include coordinates at the street-address level.

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

ArcGIS 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. ArcGIS 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

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?

ArcGIS provides ETL functions for other CMS systems that use the PII (primarily address) that is passed through ArcGIS. ArcGIS does use PII (user credentials) for system user access and authentication.

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

Not applicable.

Describe the function of the SSN.

ArcGIS does not use SSNs directly. SSNs may be part of the data that is processed through ArcGIS.

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

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

Not applicable for the user credential information of CMS employee and direct contractors maintaining the system.

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 ArcGIS system log on, where there is the CMS warning banner is presented to the system user.

All other PII that may be processed by ArcGIS is collected by IDR which is covered by it's own 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.

There is no method for a system user to opt-out of providing PII, their user credentials, because it is required for system access.

All other PII that may be processed by ArcGIS is collected by IDR which is covered by it's own PIA.

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.

All other PII that may be processed by ArcGIS is collected by IDR which is covered by it's own PIA, therefore, there is no process to notify and obtain consent by the ArcGIS system.

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.

All other PII that may be processed by ArcGIS is collected by IDR which is covered by it's own PIA, therefore, there is no process to resolve concerns by the ArcGIS system.

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

ArcGIS maintains the data integrity and availability by employing security procedures including firewalls, role based access and encryption layers. The users of the system and GIS administrators maintain data accuracy and relevancy by the following methods: users can correct their own PII data within their own EUA account; 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 ArcGIS, 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 in order to manage their user accounts.

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 Enterprise User Administration (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.

Technical controls like role-based access controls (RBAC) will allow users to only access maps based on permissions. Additionally, the maps will visualize query results for only those read-only views the user has permission for.

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).

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.

ArcGIS follows the CMS Records Schedule published in the National Archives and Records Administration (NARA) General Records Schedule DAA- GRS-2013-0006-0003, 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.