US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/06/2016

OPDIV:

CMS

Name:

Medicare Shared Savings Program Communication Dissemination Portal

PIA Unique Identifier:

P-7493548-789557

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Development

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?

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

The Medicare Shared Savings Program Communications and Dissemination Portlet (CDP) allows CMS to share information with participating Accountable Care Organizations (ACOs) and provide feedback on cost-saving efforts through reports. The CDP will offer content that is useful to the success of cost- saving efforts and provide reporting tools that allow ACOs to easily analyze and display data in a meaningful way and allow for data analysis to support ACOs' achievement of program goals, including providing better care for individuals, improving health for populations and lowering growth in Medicare Parts A and B expenditures.

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

The information collected, maintained or disseminated includes Medicare beneficiary PII such as name, date of birth, health information claim number, mailing address, phone numbers, medical record numbers for the purpose of supporting regulatory, reimbursement and policy functions of shared savings programs and to combat fraud, waste and abuse in certain health benefits programs.

For users from Accountable Care Organizations and CMS employees, user name is maintained in the CMS Enterprise Identity Management (EIDM) system. EIDM is a separate system and passes user credentials to the CDM for the purpose of providing access to the correct information. The CDM uses the EIDM created user credentials to restrict access to data the user is authorized to see.

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

The Medicare Shared Savings Program Communications and Dissemination Portlet (CDP) allows CMS to share information with participating Accountable Care Organizations (ACOs) and provide feedback on cost-saving efforts through reports which contain detailed and summary information of Medicare beneficiaries claims data. The CDP will offer content that is useful to the success of cost-saving efforts and provide reporting tools that allow ACOs to easily analyze and display data in a meaningful way and allow for data analysis to support ACOs’ achievement of program goals, including providing better care for individuals, improving health for populations and lowering growth in Medicare Parts A and B expenditures. Data from the ACOs is maintained to validate the ACO is registered to access the reports. The reports are retrieved from the Accountable Care Organization - Operational System, which is a separate system. User information to access the CDP is gathered in the CMS EIDM system. EIDM is a separate system and passes user credentials to the CDM for the purpose of providing access to the correct information. The CDM uses the EIDM created user credentials to restrict access to data the user is authorized to see.

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

Name

Mailing Address

Phone Numbers

Medical Records Number

Other - Health Identification Claim Number

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

Employees

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

Beneficiary claims information and Accountable Care Organization (ACO) eligibility and contact information will be used to support the regulatory, reimbursement and policy functions of shared savings programs and to combat fraud, waste and abuse in certain health benefits programs. Also, ACO users and CMS employee PII is collected to provide access
to data they are authorized to see.

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

N/A

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

5 U.S.C. 3, Departmental Regulations

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.

09-70-0598 Accountable Care Organization - Pioneer - Medicare Shared Savings Program

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Private Sector

To provide ACOs with information they need to meet requirements

Describe any agreements in place that authorizes the information sharing or disclosure.

All participating providers must have a Data Use Agreement (DUA) in place to be able to access the information contained in the Medicare Shared Savings Program Communication Dissemination Portal. A DUA records whose data will be shared with and what data is to be shared.

Describe the procedures for accounting for disclosures.

Accountable Care Organization (ACO) participants must sign the Data Use Agreement prior to gaining access to the Medicare Shared Savings Program Communications Dissemination Portal system. All data is provided to the ACOs via reporting and the distribution of each report is tracked. CMS monitors the distribution of the reports and can identify those ACOs that have received and those ACOs that have not received their reports.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Beneficiaries provide written consent for CMS to share their Medicare claims data with the Accountable Care Organization (ACO) when they obtain services from an ACO. Information is not collected directly from the beneficiary or the 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.

Beneficiaries who do not want to have their data shared, have the option to decline to have their data shared by signing a form or calling 1-800- MEDICARE to opt out of data sharing. Beneficiaries can contact 1-800-Medicare with questions or concerns. Information is not collected directly from the beneficiary or the user.

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

A System of Records Notice (SORN) was filed for the Accountable Care Organization - Pioneer - Medicare Shared Savings Program. The SORN is 09-70-0598. A SORN would be re- issued and providers and beneficiaries would have 30 days to provide comments.

In addition, because there is a limited number of Accountable Care Organizations (ACO), each ACO would be notified. Information is not collected directly from the beneficiary or the user.

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.

Individuals are notified annually in the Medicare
& You handbook of their right to file a complaint if they believe their privacy rights have been violated. The 1-800-MEDICARE phone number is included in the handbook and there is more information on www.medicare.gov.

When an individual calls 10800-MEDICARE, the appropriate area at CMS would work with the individual to make sure the complaint is resolved. Information is not collected directly from the beneficiary or the user.

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

Data is provided to the Accountable Care Organizations (ACOs) for their review. This way the ACO can verify the accuracy and relevancy of the data. Integrity is maintained through system security and control processes that are evaluated by independent assessors. Availability is maintained through system redundancies.

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

Users:

Review and analyze data and reports

Administrators:

To perform tasks to maintain the system

Developers:

To resolve issues and correct programming errors encountered in production

Contractors:

Serve in the role of Developers

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

Access to the systems is given based on need to know and job responsibilities to obtain reports, maintain the system or correct programming errors using a user id and role based access. Access is obtained using a CMS access request form. The form is approved by the designated approvers prior to access being granted.

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.

Access to the system is controlled using security software. The user, administrator or programmer is given the least amount of access required to obtain information and to perform their job duties, and is explicitly denied access by the security software unless otherwise granted.

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.

All administrators and developers are required to take annual CMS training regarding security and privacy requirements for protecting PII. In addition, role based training is provided to individuals with significant access or security responsibilities. This annual role based training is required by the CMS Chief Information Officer Directive 12-03.

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

In addition to the general security and privacy awareness training, users must acknowledge rules of behavior. Also, throughout the year, users are provided with newsletters, list serve messages and security bulletins.

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.

In accordance with National Archives Record Control Schedule DAA-0440-2012-0014, records containing PII will be maintained for a period of up to 6 years after the annual cutoff and destroyed in accordance with existing agency and federal government guidelines, policies and procedures.

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

Access to the system is given based on need to know and job responsibilities. The Medicare Shared Savings Program Communications Dissemination Portal system is processed in a CMS data center. CMS uses security software and procedural methods to provide “least privilege access” to grant or deny access to data based upon a need to know. External audits also verify these controls are in place and functioning. Technical controls include user identification, passwords, firewalls, virtual private networks and intrusion detection systems. Physical controls include guards, identification badges, key cards, cipher locks and closed circuit televisions.

Identify the publicly-available URL:

https://portal.cms.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes