US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/06/2016

OPDIV:

CMS

Name:

Accountable Care Organization-Operational System

PIA Unique Identifier:

P-3251671-871362

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.

The web portal was decommissioned.

Describe the purpose of the system.

The Accountable Care Organization - Operational System (ACO-OS) system gathers information on services provided by ACOs. This information is used to assess new payment and service delivery models to improve quality and reduce costs. Quality performance standards are determined by the Department of Health and Human Services Secretary and may include measures of clinical processes and outcomes, patient and/or caregiver experience and utilization measures. ACOs meeting quality standards will be eligible to receive a share of savings if costs meet documented benchmarks.

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

The information collected, maintained or disseminated includes claims data which includes information of providers and beneficiaries. It includes name, date of birth, Health Insurance Claim Number (HICN), 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 using non-financial claims data. Individual providers have the option to participate in an Accountable Care Organization. There is no user interface; therefore the system does not maintain any user data or credentials.

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

The Accountable Care Organization - Operational System (ACO-OS) system gathers claims related data from existing CMS systems and uses the data to create reporting. This information is used to assess new payment and service delivery models to improve quality and reduce costs. ACOs meeting quality standards will be eligible to receive a share of savings if costs meet documented benchmarks. An Accountable Care Organization (ACO) accesses their report via an Electronic File Transfer mailbox, which is hosted in the CMS Baltimore Data Center, or via the Medicare Shared Savings Program – Communication Dissemination Portal, which is a separate system with its own Privacy Impact Assessment (PIA). Because reporting is distributed to ACOs via other systems, the ACO-OS system has no end users. Also, because the database is maintained by the CMS Baltimore Data Center (EDC4), the administration and maintenance of the system is managed by EDC4. There are no internal ACO-OS system administrators or developer users.

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 Insurance Claim Number

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

Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Beneficiary claims information and Accountable Care Organization 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.

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.

Section 1899 of Title XVIII of the Social Security Act (42 U.S.C. 1395 et seq.)

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, ACO Database System HHS/CMS/CM and HHS/CMS/CMMI

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Non-Governmental Sources

Other

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 receive the information contained in the Accountable Care Organizations - Pioneer -Medicare Shared Savings Program system. A DUA records who 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 reports available from the Accountable Care Organizations Pioneer -Medicare Shared Savings Program 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 the 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.

The PII within Accountable Care Organization - Operational System is not collected directly from the individual but from another CMS system that contains claims data, so there is no process in place. Beneficiaries are asked to provide written consent for CMS to share their Medicare claims data with the Accountable Care Organization (ACO) when they obtain services from a provider that is associated with an ACO.

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.

The PII within Accountable Care Organization - Operational System is not collected directly from the individual but from another CMS system so there is no process in place.

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.

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 ACO Database System HHS/CMS/CM and HHS/CMS/CMMI (09-70-0598). A SORN would be re-issued and providers and beneficiaries would have 30 days to provide comments.

In addition, because there are a limited number of Accountable Care Organizations (ACO), each ACO would be notified.

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 1-800-MEDICARE, the appropriate area at CMS would work with the individual to make sure the complaint is resolved.

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.

Others:

There are no users; therefore, there is no access to this system.

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

There is no user interface for this system; therefore, no process is needed to provide access to users, administrators, developers or contractors.

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.

There are no users of the Accountable Care Organization - Operational System. Access to the data is provided via separate CMS systems.

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 system owners and developers are required to take annual CMS training regarding the security and privacy requirements for protecting PII. In addition, role based training is provided to individuals with significant responsibilities. This annual role based training is required by the CMS Chief Information Officer Directive 12-03. Also, throughout the year, CMS provides newsletters, list serve messages and security bulletins to these individuals.

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

None.

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 NARA RCS DAA-0040- 2012-0014-0001 records containing PII will be maintained for a period of up to 6 years after the annual cutoff is determined 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.

There is no access to the Accountable Care Organization-Operational System (ACO-OS). The ACO-OS system is process 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 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 used include guards, identification badges, key cards, cipher locks and closed circuit televisions.

Note: web address is a hyperlink.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.