US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/16/2016

OPDIV:

CMS

Name:

CCIIO Enrollment Resolution and Reconciliation System

PIA Unique Identifier:

P-6245546-621926

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.

Contractor

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 CMS Center for Consumer Information and Insurance Oversight (CCIIO) Enrollment Resolution and Reconciliation (CERRS) system is a case management and tracking system. CERRS was created as part of the Affordable Care Act (ACA) to reconcile discrepancies and other problems that may occur in connection with enrolling in Qualified Health Plans (QHPs) within the Federally Facilitated Marketplaces (FFM), State-Based Exchanges (SBEs) and Federally-facilitated Small Business Health Options Program (FF-SHOP).

CERRS also assists with reconciling issues with IRS tax form 1095-A, Health Insurance Marketplace Statement. This form, 1095-A, is provided to consumers who have participated in a QHP. Consumers need this form to complete and file their annual Income Tax returns.

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

For CERRS caseworkers and analysts to review and resolve both enrollment discrepancy cases and problems with the IRS 1095-A form, CERRS receives and stores/maintains information from other CMS system.

The information in the files includes: consumer full name, social security number (SSN), date of birth, mailing address, phone number, email address, healthcare insurance application ID, insurance policy ID, policy start and end dates, eligibility status, plan premium amount, and advanced premium tax credit (APTC). When applicable, the file will also contain the names, SSN and date of birth of any dependents of the consumer.

Caseworkers create case IDs, ticket numbers, and other data about problems needing reconciliation or resolution. The system also stores information about which staff analysts are assigned to which cases, the status of cases undergoing reconciliation or resolution, and the disposition of cases. In addition, resolution of some problems may require contacting QHPs to obtain supplemental information.

CERRS collects and maintains the CERRS user credentials which include first and last name, email address, a username, and password.

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

CERRS is a case management and tracking system for the resolution of discrepancies of enrollment information between the CMS FFM and either QHPs or the SBEs or FF-SHOPs. The secondary purpose of CERRS is to reconcile any problems with the IRS 1095-A form, used by consumers to complete their annual Income Tax returns. Analysis of either type of discrepancies involves using data shared from several other CMS systems with CERRS. The information transmitted to CERRS is stored for the length of time to resolve the case.

To resolve enrollment discrepancies, CERRS receives information from these systems: the Health Insurance Casework System (HICS), Multidimensional Insurance Data Analytics System (MIDAS), and Enrollment Data Baseline Outbound (EDBO). These CMS systems each have their own Privacy Impact Assessment (PIA) that addresses the PII collected and stored within those systems.

Core data elements used from these systems include: consumer full name, SSN, date of birth, mailing address, dependent names, phone number, email address, healthcare insurance application ID, insurance policy ID, policy start and end dates, eligibility status, plan premium amount, and advanced premium tax credit (APTC) amount. When applicable, the file will also contain the names, SSN and date of birth of any dependents of the consumer.

After the information is transmitted to CERRS for use in casework and analysis, it is stored in CERRS; as well as case IDs, ticket numbers, and other data about problems needing reconciliation or resolution. The system also stores information about which analysts are assigned to cases, the status of cases undergoing reconciliation or resolution, and the disposition of cases.

CERRS also manages the reconciliation of incorrect information on IRS form 1095-A. The 1095-A states the time period that a consumer participated in a QHP, FFM, SBE or FF-SHOP program. This information is required for an individual to determine whether they are exempted from owing the "individual shared responsibility payment" on their Income Tax return. It is a fine/fee for not carrying healthcare insurance as mandated by the ACA.

CMS sends 1095-A forms to consumers. If any errors or issues exist with these forms, these cases are referred to the CERRS team for resolution. Data used in 1095-A issue resolution is transmitted from HICS, MIDAS and EDBO. The information in the data file that CERRS uses includes the consumer's name, address, phone number and insurance plan-specific information such as application ID or policy ID and dates of coverage.

CERRS stores user credentials, which are the user first and last name, email address, username, and password. CERRS system users are CMS employees and direct contractors. User credentials are stored for the length of the user's employment or need to access CERRS.

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

E-Mail Address

Mailing Address

Phone Numbers

Other: Healthcare policy ID and application ID, Eligibility status, Dates of coverage, Dependent

Enrollment application data from FFM or insurers

Eligibility determination results

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

Employees

Public Citizens

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is used to help ensure that enrollment data and policy data maintained by insurance carriers, CMS, and state-based exchanges is accurate, consistent, and refers to the right individuals.

Usernames and passwords for CERRS users are used to identify and authenticate users accessing the system.

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

The secondary purpose of CERRS is to reconcile any problems with the IRS1095-Aform, used by consumers to complete their annual Income Tax returns.

Describe the function of the SSN.

CERRS uses SSNs as one of several key identifiers to link records about consumers stored in these other CMS systems HICS, MIDAS and EDBO.

Cite the legal authority to use the SSN.

Patient Protection and Affordable Care Act of 2010, sections 1411 and 1414, codified at 45 C.F.R. 155.310 and 26 U.S.C. 6103

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

Patient Protection and Affordable Care Act (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152); Affordable Care Act. Title 42 U.S.C. sections 18031, 18041, 18081-18083, and section 1414.

5 USC Section 301, 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.

Health Insurance Exchanges System (HIX), 09-70-0560 published March 6, 2013, updated May 29,

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Title: Establishment of Qualified Health Plans and American Health Benefit Exchanges

OMB No. 0938-1191, expiration date: 06/30/2019

Title: Program Integrity and Additional State Information Collections

OMB No 0938-1213, expiration date: 11/30/2016

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 to individuals occurs prior to CERRS receiving any PII. CERRS does not collect information from individuals.

CERRS users are notified at the time of hire or at the time they are assigned to the CERRS program.

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.

CERRS does not directly collect PII from consumers, so CERRS does not provide an option to 'opt out.'

CERRS users cannot opt out of providing their names, email addresses, and usernames as these data are required to create user accounts needed to access the system

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

CERRS does not directly collect PII from individuals for storage or use in CERRS. The PII CERRS uses is provided by other CMS systems, MIDAS, HICS, EDBO.

CERRS users are presented with a "warning banner" when logging into the system. Should any major changes occur, users would be notified by email or on the "welcome page".

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.

CERRS does not directly collect information from the general public, so there no process in place for this reason.

If CERRS users find inaccuracies in their PII maintained in CERRS, they can request a change or correction to this information from the CERRS Administrators.

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

CERRS receives PII about consumers from other CMS systems. CERRS relies on those systems to provide current, accurate, and relevant information. CERRS does perform file-level and record-level data integrity checks as part of the process of aggregating data received from other systems and data sources.

These procedures are both automated by the system and performed manually by CERRS database administrators. Periodic reviews of information contained in the system, including PII, are performed at regularly scheduled intervals and at milestone dates such as the end of open enrollment for insurance plans offered through exchanges. Data accuracy and relevancy are reviewed and validated by case analysts, on an ongoing basis, as part of the core casework activity involved in resolving cases; since the reason that most cases are referred to CERRS have data inconsistencies, errors, or discrepancies that must be resolved.

CERRS system administrators review user account information for relevancy and accuracy at least every six months.

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

Users:

CERRS users require access to PII to perform case analysis and issue and resolution activities related to consumer records.

Administrators:

Caseworker administrators require access to PII because they process data files containing consumer records received by CERRS. System administrators require access to PII to maintain and control the access to CERRS.

Contractors:

CERRS users and administrators are direct contractors, so their work with CERRS requires access to PII as described in the User and Administrator roles.

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

The administrative procedures in place to determine which system users may access PII are authentication and authorization rules that give specific permissions to each user role. The role-based access is based on the principle of 'least privilege' where users are given 'need to know' and 'need to access' permissions. All user roles and authorizations for the system are documented in the CERRS System Security Plan (SSP). Access to PII requires authentication to CERRS and authorization via the CERRS Active Directory of authorized users.

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.

The system controls in place for access to PII include role-based access permissions, and limits on the PII that is displayed so that only the minimum amount of PII is visible to users. Within CERRS, users are assigned different roles corresponding to different levels of access to data as well as the ability to perform specific actions (e.g., read, update, delete).

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 CERRS personnel undergo corporate and project-specific training at time of hire and annually thereafter. This training includes security and privacy awareness training with content specific to the protection of PII and Protected Health Information (PHI) and other sensitive or confidential information. CERRS personnel also must complete project-specific training before starting work on the project or receiving access to CERRS. All personnel must sign agreements to acknowledge awareness of their responsibilities to protect this information.

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

CERRS personnel must complete additional two weeks of full-time project-specific training before starting work on the project or receiving access to CERRS. Training courses include content about correct use of CERRS as well as how to conduct case analysis and other project activities performed using the system.

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.

PII within CERRS records is maintained only as long as needed to support reconciliation or resolution of cases, or to satisfy retention policies established for the Federally Facilitated Marketplace. CERRS will maintain case records for 10 years. Records management adheres to CMS standards and procedures and to National Archives and records Administration (NARA) General Records Schedules 20 (Electronic Records) and 24 (IT Operations and Management Records).

Destruction of PII in hard copy and electronic form conforms to procedures and standards for media sanitization specified in CMS Minimum Security Requirements.

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

CERRS implements all security and privacy controls and enhancements specified in the CMS Minimum Security Requirements for systems containing PII. All controls are fully documented in the CERRS System Security Plan.

Administrative controls implemented for CERRS include access control such as passwords so that only authorized users can access the system, role-based access for registered users, and maintaining audit logs of users activities within CERRS.

Technical controls implemented for CERRS include firewalls, anti-virus and intrusion detection tools, vulnerability scanning, and encryption of data in transit.

CERRS is located within a CMS data center facility where physical controls implemented include locked doors requiring access cards for entry, video cameras, and security guards that monitor building access and activity.

Note: web address is a hyperlink.