US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/16/2016

OPDIV:

CMS

Name:

Marketplace Consumer Record

PIA Unique Identifier:

P-5453163-100531

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 purpose of Marketplace Consumer Record system (MCR) is to provide a database of consumer information to improve the consumer experience and reduce operational costs of Federally Facilitated Marketplace (FFM) consumer data for CMS organizations. MCR makes available the complete enrollment and eligibility data to respond to consumer inquiries during or after the initial application and/or enrollment period in the FFM.

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

MCR aggregates the following enrollment information about consumers that enroll in the FFM: full name, date of birth, Person Tracking Number (PTN), Taxpayer ID, email address, mailing address, telephone number, household income, employment information, healthcare insurance plan identification number and Social Security Number (SSN).

MCR retrieves this information from the following CMS FFM Eligibility & Enrollment (FFM & E&E) databases: Next Generation Desktop (NGD), Eligibility Appeal Case Management System (EACMS), Health Insurance Casework System (HICS), Consumer Enrollment Resolution and Reconciliation System (CERRS), and the Eligibility Support Workers (ESW) Clearing House Database. Each of these systems is responsible for the security and privacy measures put in place to protect the information within them and each has its own PIA.

MCR system administrators log into MCR utilizing their CMS access credentials, 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.

The MCR system is an internal CMS system that retrieves and aggregates consumer information from the FFM E&E databases. MCR enables other CMS programs to directly answer consumer questions about their healthcare coverage enrollment; identify and resolve enrollment discrepancies, assists with the reduction in the length of time to resolve issues and more quickly evaluate and make accurate enrollment and appeals decisions.

The MCR system supports the following CMS programs: ESW, FFM Call Center Representatives (CCR), CMS Regional Office Account Managers and Caseworkers, Appeals Workers, and 1095A Discrepancy Resolution & Enrollment Reconciliation Workers.

The consumer information transferred to and stored in MCR is retained permanently, subject to any updates or changes to the information.

MCR system users and administrators are CMS direct contractors who log into MCR utilizing their CMS username and password. This user information is maintained for as long as the user requires access to MCR.

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

Employment Status

Taxpayer ID

Other - Username and password; Person Tracking Number (PTN); healthcare insurance plan

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?

The primary purpose of PII in the MCR system is to initiate search functions to locate consumer's data. System user PII is used for account creation and access to MCR.

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

N/A

Describe the function of the SSN.

The SSN is used to validate an individuals' identity within the MCR system.

Cite the legal authority to use the SSN.

42 U.S.C. Section 18081
Affordable Care Act (ACA), Section 1414
Affordable Care Act (ACA), Section 1411

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

42 U.S.C Section 18081
Affordable Care Act (ACA), Section 1414
Affordable Care Act (ACA), Section 1411
5 U.S.C. 301, Departmental Regulation

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.

09-70-0560 Health Insurance Exchange Program (HIX), published February 6, 2013, and updated

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

CMS Form Number: CMS-10400 Title: Establishment of Qualified Health Plans and American Health Benefit Exchanges OMB control number: 0938-1156 Expiration Date: 06/30/2019

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.

There is no process in place to notify individuals that their personal information will be collected because MCR system retrieves PII data from other FFM E&E information systems. Those systems are responsible for notification to Individuals.

For the MCR system users, a warning banner is displayed upon each log-in notifying that personal information will be collected.

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 in place for individuals to opt-out of the collection or use of their PII within MCR. PII stored within MCR is not collected by MCR. The PII is collected from the individual by FFM E&E systems.

MCR system users cannot opt out of PII collection (their username and password) 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.

There is no process to notify and obtain consent from the individuals whose PII is stored by MCR if a major change to the system occurred because the PII is collected by the FFM E&E databases.

MCR system administrators would be notified by normal CMS methods of warning banners, or email notification.

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 an individual has a concern about their PII, the process to report a PII related issue is to contact the Health Insurance Marketplace call center at 1-800-318-2596 and describe the concern. The call center would investigate and work with the individual to resolve their concern. MCR is one of the databases that support the call center for that purpose.

MCR system users would contact the CMS IT help desk and the help desk would investigate the issue and determine if further action is needed.

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

As part of CMS, MCR is part of the CMS continuous monitoring process based on the National Institutes of Science and Technology (NIST) recommendations to ensure system integrity, availability, accuracy and relevancy. The program is reviewed annually.

MCR and the FFM E&E database are designed with logic checks to ensure data accuracy, availability and integrity. The CMS Center for Consumer Information and Insurance Oversight (CCIIO) is required to review and update the enrollment process on a yearly basis to ensure that all data collected is relevant to the health insurance enrollment process.

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

Administrators:

MCR system administrators may have access to PII as part of their maintenance support activities.

Contractors:

CMS direct contractors in their role as system administrators may have access to PII as part of their role as an administrator.

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

Individuals requesting access to MCR must sign an account request form prior to account creation account request form must indicate access level needed. This form is reviewed and approved by MCR managers. MCR uses the principle of least privilege to ensure system administrators are granted access on a "need- to-know" basis.

Only validated administrators have access to MCR. Managers must approve all system access and re-certify that access within every 365 days.

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.

Only validated administrators have access to MCR and the access is re-certified every 365 days. MCR uses role based access control to ensure system administrators are granted access on a "need-to-know" and "need-to- access" commensurate with their assigned duties.

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 contractor personnel who access or operate a CMS system are required to complete the annual CMS Security and Privacy Awareness Training course. Direct Contractors also complete their annual corporate security- related awareness training. Personnel with privileged access must also complete role- based security training commensurate with their assigned duties and receive additional job related training by attending conferences, forums, and other specific training on an annual basis.

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

N/A

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.

Records will be maintained until they become inactive, at which time they will be retired or destroyed, which is ten years. These procedures are in accordance with published records schedules of the Centers for Medicare & Medicaid Services as approved by the National Archives and Records Administration General Records Schedule 3.2 (GRS 3.2) for electronic records.

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

Administrative controls such as written policy, procedures and guidelines have been established. System users are required to take annual Security and Privacy awareness training. Third-party assessments are done to validate the implementation of the system controls that have been implemented to prevent unauthorized access, to safeguard the data in the event of a disaster, and to audit activity within the application.

The technical controls in place are firewalls and encryption to prevent unauthorized access. Other technical controls include security scans, penetration testing, intrusion detection and prevention systems (IDS/IPS) and computer system controls that prevent users without administrative or developer access to log into a test environment and the test environment and usable application are not joined together.

The physical controls in place are that servers are located in a secured data center with surveillance cameras, security guards, locked rooms, locked server cabinets, a network operations center, and security desk with visitor logs for controlled access.