US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/29/2016

OPDIV:

CMS

Name:

Marketplace Outreach Data System

PIA Unique Identifier:
P-1838448-130005

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 Marketplace Outreach Data System (MODS) is a CMS internal application which compiles consumer contact data from the Multidimensional Insurance Data Analytics System (MIDAS), GovDelivery, and the CMS Call Center into an analytics database. The information is used for targeted outreach (communication) efforts and research on the effectiveness of outreach efforts in connection with consumers who have expressed interest in enrolling in or begun the process of enrolling in the Federally Facilitated Marketplaces (FFM).

Describe the type of information the system will collect, maintain (store), or share.
MODS receives information from both MIDAS and GovDelivery on a daily basis through a secure Electronic File Transfer (EFT) method and information on a weekly basis from the CMS FFM Call Center.

MODS receives daily snapshots of the following data from MIDAS about the people seeking health insurance on the FFM website, healthcare.gov.

Contact information, which includes: name; email address; phone number; and mailing address. Account information, such as: account creation date and last login date. Application information, such as: date of birth, application creation date, application submission date, cost-sharing reduction eligibility and tax credit eligibility information. Insurance plan information, such as: insurer, plan coverage level, plan start date, and plan end date.

MODS receives snapshots, every two hours, of the following data from CMS email vendor GovDelivery: Subscriber data about people seeking health insurance on the FFM, including email address; and date subscribed and date unsubscribed; and Analytics data about emails received from GovDelivery to subscribers including the date the person opened the email and date they clicked a link in an email.

MODS receives weekly snapshots of the following data from CMS' call center: the caller's name, phone number, call time and duration, and call result, such as whether the person was directed back to the FFM website.

MODS transfers targeted lists back to GovDelivery for outreach as instructed by CMS Office of Communication (OC). These lists may include the following data. Contact information of consumers seeking health insurance on the FFM, including name, email address, phone number and language preference. Geographic information about the consumer, such as a zip code or parts of the mailing address (city and state).

MODS transfers targeted lists to the CMS Call Center for outreach as instructed by CMS OC. These lists may include the name, phone number and language preference of those consumers seeking healthcare coverage through the FFM.

To access MODS, system users must provide user credentials: a user ID and password. System users are CMS employees and CMS direct contractors.

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

MODS compiles information about consumers who have expressed interest in enrolling in or started to enroll in the FFM through the healthcare.gov website. The information is provided to MODS by other CMS systems, MIDAS, GovDelivery and the CMS FFM Call Center. The information is used for targeted outreach (communication) efforts and research on the effectiveness of outreach efforts with consumers.

The information received by MODS, from both MIDAS and GovDelivery, is on a daily basis through a secure Electronic File Transfer (EFT) method and on a weekly basis from the CMS FFM Call Center. This is consumer information, such as contact information, including geographical; and communication information, email correspondence, about consumers. All three of these systems have PIAs to address the PII that is collected, maintained and shared by those systems with MODS.

MODS creates lists from the data that are transferred back to GovDelivery and the Call Center on a daily or weekly basis to enable them to contact people seeking health insurance on the FFM. These communications are ongoing throughout the year, and especially during Open Enrollment for healthcare. They are to help consumers understand when and how to choose the best coverage for their individual circumstances, and how to maintain and use that coverage throughout the year.

The MODS data is incorporated into reports and analysis used by the Office of Communication to continuously measure, assess the effectiveness of, and improve outreach performance; and to study and understand users' knowledge and behavior when engaging with the FFM website, healthcare.gov.

To access MODS, system users input user credentials for system access.

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

E-Mail Address

Mailing Address

Phone Numbers

Other: User ID and password; Language preference

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 produce lists for outreach via email, SMS, and outbound phone calls. PII is also used for system login by system users.

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

PII is also used to report on and analyze the effectiveness of outreach activities.

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

Patient Protection and Affordable Care Act, 42 U.S.C. § 18001 (2010); 5 USC 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 (HIX), 09-70-0560, published 2/6/2013 and updated 5/27/2013 and 10/23/2013.

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

Private Sector

Identify the OMB information collection approval number and expiration date

0938-1190, expiration date 3/31/2020
0938-1191, expiration date 6/30/2019

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.

Since MODS does not directly collect PII from consumers, to there isn't a method to notify them that PII is collected. MODS receives consumer PII from GovDelivery and MIDAS, those systems are responsible for notifying individuals that their PII is collected.

The system users are notified at system login by a banner notice that their PII (user credentials) is being 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 for MODS users to opt-out of providing their PII to access the system as it is required to utilize the system. Since MODS does not directly collect any PII from consumers, but from MIDAS and GovDelivery, those systems are responsible for opt-out methods.

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

MODS does not have a defined process to notify and obtain consent from the individuals whose PII is in the system when major changes occur because the data is inherited from MIDAS and GovDelivery. Those systems are responsible for notifying and obtaining consent from individuatls. For MODS system users, they would be notified by email and CMS announcements.

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.

MODS does not directly interact with consumers, so there isn't a process in place if a consumer has concerns about their PII. They would contact the CMS FFM Call Center. For system users, they would contact the CMS IT Help Desk by email or telephone. The Help Desk would investigate and determine if there is an issue and elevate it to the appropriate CMS department for resolution.

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

There is not a defined process for periodic reviews of PII in MODS because the data is inherited from MIDAS and GovDelivery. The PII is transferred on a daily and weekly basis from MIDAS and GovDelivery and that process would inherently update any information as those systems would update and change any PII to ensure the integrity, availability, accuracy and relevancy. MODS does receive and store PII in secured formats.

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

Administrators:

Administrator access is required to ensure MODS is functioning properly.

Developers:

Developer access is required to ensure the data pipeline is functioning properly.

Contractors:

CMS' direct contractors, in their roles as administrators, developers and analysts, would have access to PII to perform the job functions of those positions.

Others:

Analysts require access to conduct data analysis and run reports

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

MODS uses role-based access controls to ensure that administrators, developers and analysts are granted access on a ‘least privilege’ basis, so that only those with the "need" to access the system are granted access for their assigned task/duties only.

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.

MODS uses role-based access controls to ensure that administrators, developers and analysts are granted access on a ‘least privilege’ Specifically, only administrators have access to all environments; analysts only have access to the database information but cannot edit or modify it; and developers will only have access to programing and related information.

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 MODS users are required to take the CMS Information Security and Privacy training on an annual basis, or whenever changes to the training module have been made. This training includes details on the handling of PII.

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

CMS employees and contractors with privileged access are required to complete role-based training and meet continuing education requirements commensurate with their role. Other training such as conferences, seminars and classroom training provided by CMS/HHS is available apart from the regular annual training.

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.

Data in MODS is maintained indefinitely at this time.CMS record retention guidelines are specified in the CMS Records Schedule published in April 2015 and reference the the National Archives and Records Administration (NARA) Records Control Schedule (RCS) N1-440-10-006, which states that records will be destroyed or deleted after between 2 and 5 years, or longer if needed by CMS for the resolution of claims, audits or other purposes.

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

Access is restricted to a small set of users. Users must be whitelisted (approved) by CMS, and have a CMS user account. Users can only access the system from an approved Internet Protocol (IP) address.

Technical controls include encryption of transmitted and maintained infomation, the use of intrusion detection and prevention technologies and multifactor authentication to access the system.

The system is located within a CMS certified data center with physical controls, such as limited access to the building, the presence of security guards and video monitoring.