

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/19/2016

OPDIV:

CMS

Name:

CO-OP Program Management System

PIA Unique Identifier:

P-1420367-352598

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?

Yes

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 Consumer Operated and Oriented Plan (CO-OP) program was established as part of the Affordable Care Act (ACA). The purpose of the program is to foster the creation of qualified nonprofit health insurance issuers to offer competitive health plans in the individual and small group markets. The program awards start-up and solvency loans to approved CO-OP Issuers and monitors the start-up, licensure, and compliance of the CO-OP Issuers.

The CO-OP Program Management System (CPMS) is designed to support the mission of the CO-OP program and is the primary tool to be used by the CMS Account Managers (AMs) to record and track the progress of each individual CO-OP Issuer's start-up and operational activities, including their loan disbursement and repayment.

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

CPMS collects the following data items: user ID and password from internal CMS Operations Division users, direct contractors and external users (state-based CO-OP Issuers) in order to log into the system. All users required HHS provided credentials to access the system.

CPMS also collects the following CO-OP information: Insurance issuer's business name, business address, office phone number, and website address.

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

CPMS is a record-keeping system for CO-OP Issuers, providing management tracking, financial tracking (loan agreement), risk and issue tracking, and reporting. CPMS is used by both internal CMS users and CO-OP Issuer users. CPMS tracks CO-OP Issuer milestones for standing up the organization and is used as a tool to submit, review and approve disbursement requests (start up and solvency) and milestone extension requests. CPMS is the primary tool used by CMS Account Managers to communicate with CO-OP Issuers.

CPMS also collects the following CO- OP information: Business name, business address, and office phone number, and website address. Those information are collected to help CMS Account Managers (AMs) to record and track the progress of each individual CO-OP Issuer's start-up and operational activities, including their loan disbursement and repayment. The business information collected (Business name, business address, office phone number, and website address), helps to identify CO-OP Issuers not individuals working for the CO-OP Issuers.

CPMS also collects user ID and password from internal CMS Operations Division users, direct contractors and external users (state-based CO-OP Issuers) in order to log into the system. However these login credentials(User Id and Password) are provided to users by another CMS system which is Collaborative Application Lifecycle Tool (CALT), which is covered by another Privacy Impact Assessment (PIA).Users need to be created in CALT first before they can be granted access to CPMS.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

Mailing Address

Phone Numbers

Other - Business name, business address, office phone number, and website address. Login

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

User ID and password (Login credentials) are collected by CPMS to allow users (internal CMS users and external CO-OP Issuer users) to log into the system in order to record and track the progress of each individual CO-OP Issuer's start-up and operational activities, including their loan disbursement and repayment. User name and password are provided by another CMS system which is Collaborative Application Lifecycle Tool (CALT).

The business information collected (Business name, business address, office phone number, website address), helps to identify CO-OP Issuers not individuals working for the CO-OP Issuers.

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.

Title 42 U.S.C. 18031, 18041, 18081—18083
and section 1414 of the Affordable Care Act; 5
U.S.C. 301 Department 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) Program, 09-70-0560

SORN is In Progress

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

N/A for user credentials.

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.

CPMS collects CO-OP information (CO-OP name, business address, office phone number, website; CO-OP contact work email address and work phone number). CPMS login page contains language stating that by using the system, users understand and consent to the following terms of use: "You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system."

CPMS also collects user ID and password from internal and external users in order to log into the system. However these login credentials (User Id and Password) are provided to users by another CMS system which is Collaborative Application Lifecycle Tool (CALT). Users need to be created in CALT first before they can be granted access to CPMS. CALT PIA provides the process that notifies individuals that their 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.

Information collected on CO-OPs (CO-OP name, business address, office phone number, website; CO-OP contact work email address and work phone number) is based on the information they provided in their account details. These are not required fields, so the user can remove them whenever they deem necessary and choose to opt out.

Potential user cannot 'opt-out' of providing login credentials (user ID and Password). The login credentials are needed to grant access to CPMS.

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

For the information collected on CO-OPs (CO- OP name, business address, office phone number, website; CO-OP contact work email address and work phone number) at present there has been no major changes to the system regarding disclosure or data uses, however at the point in time when there is a change, all system users will be notified regarding the change and request their consent.

The login credentials within this system are provided to users by another CMS system which is Collaborative Application Lifecycle Tool (CALT). CALT PIA addresses the process to notify and obtain consent from the individuals.

CPMS login page also contains language stating that by using the system, users understand and consent to the following terms of use: "You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system."

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 believes their PII has been inappropriately obtained, their first step is to contact the CMS Exchange Operations Support Center Help Desk at 1-855-CMS-1515. The help desk staff will then pass this complaint on to the business owner in the CMS CO-OP Program Office, who will then work with both the user and the developer team to remove or correct the information as 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.

For business contact information within CPMS, back-up servers are in place to ensure information is readily available, even if a main server fails. Users receive an annual email requesting that they review their information and ensure that it is accurate and up-to-date.

Relevancy is ensured through monthly audits of user accounts and removal of any inactive accounts. Lastly integrity is ensured using the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access to business contact information on a "need-to-know" and "need-to-access" commensurate with their assigned duties.

The login credentials within this system are provided to users by another CMS system, which is Collaborative Application Lifecycle Tool (CALT). CALT PIA addresses the periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

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

Users:

CMS Account Managers (AMs) access CPMS to record and track the progress of each individual CO-OP Issuer's start-up and operational activities, including their loan disbursement and repayment.

CO-OP Issuers access CPMS to submit request, track the progress and activities of their individual accounts.

Administrators:

Administrators (CMS employees and direct contractors) require access to operate and maintain the system. They also have the ability to create and modify user account.

Contractors:

Direct contractors as administrators require access to operate and maintain the system. They also have the ability to create and modify user account.

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

Prospective users of CPMS must sign an account request form. The account request form must also be filled indicating the minimal access required to perform one's tasks. Users and their roles are reviewed and approved by the business owner before access is granted to CPMS. Each time a new user is requested, the business owner reviews the request and makes a determination whether to permit access.

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.

CPMS uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties. System Administrators review user accounts at least annually. Any anomalies are addressed and resolved by contacting the user, and modifying their user data, or by removing their access if no longer required. Activities of all users including system administrators are logged and reviewed by CPMS ISSO to identify abnormal activities if any.

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 CPMS users are required to complete the annual CMS Security and Privacy Awareness training provided annually as Computer Based Training (CBT) course. Individuals with privileged access must also complete role-based security training commensurate with the position they are working.

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

Direct contractors also complete their own annual corporate security 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.

System. Records are housed in both active and archival files in accordance with CMS data and document management policies and standards including GRS 3.2. National Archives and Records Administration (NARA), General Records Schedule (GRS) 3.2 states that CPMS will destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the Certification Authority, or when no longer needed for business, whichever is later.

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

Prospective users of CPMS must sign an account request form. The account request form must also be filled indicating the minimal access required to perform one's tasks. Users and their roles are reviewed and approved by the business owner before access is granted to CPMS.

CPMS uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties. System Administrators review user accounts at least annually. Any anomalies are addressed and resolved by contacting the user, and modifying their user data, or by removing their access if no longer required. Activities of all users including system administrators are logged and reviewed by CPMS ISSO to identify abnormal activities if any.

The CPMS system is located in a Tier-1 network data center (HP Virtual Data Center in Tulsa, OK) which provides premier physical control protections. Physical controls are in place such as security guards ensure that access to the buildings is granted to authorize individuals. Identification of personnel is checked at the data center.

The CPMS system is built using industry best practices and independently reviewed against Federal Information Security Management Act (FISMA) and National Institute of Science and Technology (NIST) Security and Privacy controls to ensure technical, operational, and management controls are properly applied.

Identify the publicly-available URL:

<https://cpms.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.

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?

No

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

null