US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/16/2016

OPDIV:

CMS

Name:

Medicaid and CHIP Program System

PIA Unique Identifier:

P-5080182-650000

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.

No PHI or PII has been introduced to the system. Changes only apply to system design and removal of a COTS product.

Describe the purpose of the system.

The Medicaid and CHIP (Children's Health Insurance Program) Program system (MACPro) is used by both State and CMS officials to improve the State application and Federal review processes, improve Federal program management of the Medicaid and CHIP programs, and standardize Medicaid program data. MACPro automates the process for States to submit and amend their Medicaid State Plans, Medicaid waiver programs, CHIP plan information, and State Medicaid Health Information Technology Plans (SMHPs).

Additionally, MACPro automates the uploading of States' planning documents (SPD), State Plan Amendments (SPA) and Advanced Planning Documents (APDs), as well as applications and amendments to their Medicaid and CHIP demonstrations, and grant programs.

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

The MACPro system collects and stores Medicaid and CHIP program information such as reports on the quality of care; amendments to the Medicaid and CHIP programs within each state; amendments to the administration and benefits, waiver program, types of medical care delivery systems, payment methods and other related operational information. It does not include any details or identifying information about beneficiaries or providers.

The MACPro system is accessed through the CMS portal, the Enterprise Identity Management system (EIDM). EIDM is the access control for MACPro; a MACPro user enters their user ID and password into the EIDM portal and is connected to MACPro. EIDM maintains its own PIA that outlines the security and privacy parameters for the information contained within it.

MACPro stores the user's contact information, which includes the following information: name, mailing address, position in State/Federal government, MACPro role, work email address, and work phone number. It also stores the user's username. MACPro system maintainers access the backend through servers and do not enter any user ID or password into MACPro. MACPro users are authorized state employees, 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.

The MACPRO automates the process for States to submit and amend their Medicaid State Plans, Medicaid waiver programs, CHIP plan information, and State Medicaid Health Information Technology Plans (SMHPs). This provides the mechanism for CMS to review and approve any changes to the functions of the programs such as the quality of care; amendments to the Medicaid and CHIP programs within each state; amendments to the administration and benefits, waiver program, types of medical care delivery systems, payment methods and other related operational information.

MACPro uses the CMS EIDM system for user authentication. The user is authenticated by EIDM and accesses MACPro from EIDM. MACPro contains contact information of the users to communicate between the states and CMS. MACPro system users are authorized state employees and CMS employees and contractors.

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

Yes

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

Name

E-Mail Address

Phone Numbers

Other - job position, User ID and password

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?

500-4,999

For what primary purpose is the PII used?

The PII is used for MACPro users to access the system and for the system to send communication and notification to the users.

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

Not applicable

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

5 U.S.C. 301, Departmental Regulations

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

OMB 0938-1188; 8/31/2019

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 notification by MACPro that personal information is being collected. The notification occurs at the EIDM new user registration screen and then subsequently at the user access screen of EIDM. System maintainers and administrators do not log into MACPro to perform system functions.

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 to opt-out of providing PII by individuals to access MACPro. PII, user ID, is required to access MACPro to use it. There are Terms and Conditions displayed prior to accessing MACPro advising that the individual is accessing a U.S. Government system and that there is no reasonable expectation of privacy.

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

If there were major changes to the MACPro system, the system users would be notified by warning banners on EIDM and on the informational page of the Medicaid[.]gov MACPro page through a new user access manual.

System maintainers and Administrators would be notified by CMS communications, such as email.

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.

Since an individual creates an account and accesses MACPro through EIDM, the MACPro system does not have a process to resolve an individual's concerns. An individual would contact the EIDM Help Desk by email to report their concerns. The EIDM Help Desk would investigate and assist the user and also contact the MACPro Help Desk to advise on the issues.

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

Every time a user successfully logs into MACPro via EIDM using his/her EIDM user id & password, EIDM passes the PII information (name, mailing address, MACPro role, work email address, and work phone number) of the user via header information. In order to maintain the accuracy, and relevancy of the PII stored within MACPro database, the PII information of the user is updated in the MACPro database with the new PII information that is passed onto MACPro application via header information, every time the user successfully logs into MACPro.

Under this process, all outdated, unnecessary, irrelevant, and inaccurate PII is identified and deleted from MACPro database. The PII is available as needed, and is sufficient (minimum required) for the purposes needed. The PII fields are locked and cannot be changed; the process to ensure that individuals who provide or modify PII cannot repudiate that action is done within the source (EIDM) system. The process to ensure PII is available when needed is by updating the information in MACPro with EIDM information, every time the user successfully logs into MACPro; the process to ensure that PII is sufficiently accurate for the purposes needed is ensured when the updates are sync.

Users, can at any time, request that their PII (access) be deleted, by contacting MACPro Helpdesk, who in turn, would take the corresponding action with EIDM and development teams. Accounts can be disabled for non-activity or terminate .those accounts that have not been used at least once every 366 days are deleted.

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

Administrators:

Administrators, have access to PII for user communications, system maintenance, and user account management and as necessary
for other system administration functions.

Contractors:

CMS direct contractors, in their role as a system administrator, will have access to PII information for user communications, system maintenance, and user account management.

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

MACPro uses role-based access to determine access to PII. MACPro users request access and then the CMS MACPro administrators approve the request to permit different levels of access, dependent on the assigned role.

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.

MACPro has a default 'user' role that limits the access to PII to only the users. Then the user requests additional role(s) and the MACPro administrators will approve the request based on the principle of least privilege. The additional role a user requests is pre-determined so that the user doesn't actually have choices.

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.

For all CMS employees and direct contractors, it is mandatory to complete the annual Security and Privacy Awareness training. At the end of the course, there is an examination and a certificate of completion is provided as
evidence.

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.

MACPro follows the National Archives and Records Administration (NARA) General Records Schedule (GRS) 3.1, which states that records will be destroyed after five years. The Medicaid and CHIP program information follows the CMS Records Schedule Section V. Medicaid, G. Medicaid State Plans & Amendments. It outlines several schedules that range from destroy "when no longer needed" to up to retaining for seven years and then destroying the records.

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

The administrative controls in place to secure the PII include role-based access and permissions, periodic review of users and deletion of non-active accounts.

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

The MACPro system is hosted in a secure data center that employs physical controls and monitoring to restrict physical access and ensure the security of doors with the use of security cards and pass codes; the efficacy of heating and air conditioning, smoke and fire alarms, and fire suppression systems; and by employing cameras, fencing and security guards.