

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/02/2026

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?

Yes

Identify the operator.

Contractor

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

System Re-authorization

Describe in further detail any changes to the system that have occurred since the last PIA.

Medicaid and CHIP (Children's Health Insurance Program) Program (MACPro) Appian
No major changes. All changes are normal system maintenance updates.

Children's Health Insurance Program Annual Reporting Template System (CARTS)
No major changes.

Statistical Enrollment Data System (SEDS)
No major changes.

Managed Care Reporting (MCR)

No major changes.

Quality Measures Reporting (QMR)

No major changes.

Money Follows the Person (MFP)

Newly added application since the last PIA. MFP now allows saving and submission of report data.

One Medicaid and CHIP Program System (OneMAC)

OneMAC system was upgraded and moved to a new application and architecture to continue to make it usable going into the future.

Managed Care Review (MC-Review)

This is the first PIA completed for this project. Newly added application since the last PIA.

eRegulations (eRegs)

Integration with CMS IDM Okta. Center for Medicaid & CHIP Services (CMCS) employees and contractors can request reader, editor, or admin user roles via the EUA job code system. EUA job code applications are reviewed and approved or rejected by the CMS Product Owner for this application.

Home & Community Based Services (HCBS)

Newly added application since the last PIA. HCBS now allows saving and submission of report data.

Describe the purpose of the system.

Medicaid and CHIP (Children's Health Insurance Program) Program (MACPro) Appian
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).

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.

Children's Health Insurance Program Annual Reporting Template System (CARTS)

The Children's Health Insurance Program (CHIP) Annual Reporting Template System (CARTS) is a web-based application used by the Centers for Medicare and Medicaid Services (CMS). Section 2108(a) and Section 2108(e) of the Social Security Act (SSA) provides that the states must assess the operation of their state child health plan each fiscal year, and report to the Secretary by January 1 following the end of the fiscal year, on the results of the assessment. In addition, the state must assess the progress made in reducing the number of uncovered, low-income children. National Academy for State Health Policy (NASHP) assists the states and CMS in coordinating efforts to continually analyze Title XXI annual reports for the defined purposes.

Statistical Enrollment Data System (SEDS)

The primary activity of the MACPro Data Collection Tool (MDCT) Statistical Enrollment Data System (SEDS) application is to create an information system to track and report on the Children's Health

Insurance Program (CHIP) quarterly and annual enrollment numbers.

Managed Care Reporting (MCR)

MCR is the CMS MDCT reporting application for collecting state-reported data related to Medicaid Managed Care program reports, including Managed Care Program Annual Report (MCPAR), Medical Loss Ratio (MLR), and Network Adequacy and Access Assurances Report (NAAAR). It stores the templates for the three reports, as well as a help page to reach the MDCT help desk. Users access the application via Identity Management System (IDM) and are assigned roles that correspond to their permissions. State users can enter report data and submit data to CMS.

Quality Measures Reporting (QMR)

MDCT-QMR contains web forms for states to input information about their collected data regarding Medicaid and CHIP:

Edit: Edit the annual measures based on State and Year selected.

Submit: Submit the annual measures based on State and Year selected.

View: View the annual measures based on State and Year selected.

Export measures to a PDF: Export the answers for the state and year selected to a PDF.

Money Follows the Person (MFP)

MFP is the CMS MDCT reporting application for collecting state-reported data related to Medicaid Money Follows the Person program reports, including MFP Work Plan (WP), and MFP Semi-Annual Progress Report (SAR). It stores the templates for the three reports, as well as a help page to reach the MDCT help desk. Users access the application via IDM and are assigned roles that correspond to their permissions. State users can enter report data and submit data to CMS.

One Medicaid and CHIP Program System (OneMAC)

The core function of the OneMAC Foundations application is to establish an automated information system, aimed at replacing the existing manual procedure for submitting, reviewing, and adjudicating State Plan Amendments (SPAs) and Policy Waivers, which currently relies on email-based processes. This innovative system offers a unified platform for submission and review, effectively linking metadata with SPA and Waiver submissions.

Furthermore, the system plays a pivotal role

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

MACPro (Appian)

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.

MACPro stores the user's contact information, which includes First/Last name, Email, Phone number, CMS users Group/Division, MACPro role and attributes that drive user access to MACPro functionalities.

CARTS

The system AWS accounts will collect, store, and share the same data previously collected, stored, and shared within the existing AWS account. Other than the AWS account, there will be no changes to how the data is stored nor any new data types.

Statistical Enrollment Data System (SEDS)

States record their enrollment numbers by age range on a quarterly basis at the end of each fiscal quarter as well as annually at the end of the fiscal year. This system is complementary to the MDCT CHIP Annual Report Template System (CARTS). SEDS converts an existing paper data collection process into web-based application. It also is designed to provide the reporting and exporting of survey answers into a PDF template.

Managed Care Reporting (MCR)

The system stores all saved and submitted report data and respective timestamps, along with the name associated with the IDM profile which undertook the action. This data is stored indefinitely.

Quality Measures Reporting (QMR)

MDCT-QMR contains web forms for states to input information about their collected data regarding Medicaid and CHIP.

Money Follows the Person (MFP)

The system stores all saved and submitted report data and respective timestamps, along with the name associated with the IDM profile which undertook the action. This data is stored indefinitely.

One Medicaid and CHIP Program System (OneMAC)

First name, Last Name, Company Email, Generic information related to Medicare and Medicaid requests, rewards and statuses.

MC-Review

Authorize client credentials, stored until manually deleted.

session data: stored temporarily for the duration of a user's session

This app indefinitely stores:

User account information: full name, IDM role, division assignment and email address.

When users need to lose access to the system their IDM roles are revoked.

All contract and rate submission form field inputs, uploaded documents and documents meta data. Documents may include questions and answers, and rating information including financial or contract specific information. Contact data on submissions may include full name, title, email address, and actuarial firm name.

System configuration settings, such as email notification settings, help desk contact information, and file storage URLs.

Submission activity and audit information such as submission history, user activity logs, document access logs etc. All error logs.

eRegulations (eRegs)

This application indefinitely stores:

Text and metadata of public regulations and Federal Register documents, retrieved from public Application Program Interface (API)s offered by eCFR.gov and the FederalRegister.gov.

Metadata about policy-related documents published by CMS, HHS, and other public sources relevant to Medicaid & CHIP, entered by contractors on this team.

Credentials for contractors who edit document metadata in this application: username created by a system administrator, and a password created by a system administrator and then immediately changed by the individual. When a contractor leaves the project, a system administrator deactivates the account; the username remains in the system, but the individual cannot log into the account. There are fewer than 15 accounts in this application.

Home & Community Based Services (HCBS)

The system stores all saved and submitted report data

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

MACPro (Appian)

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 currently collects, maintains, or shares the following information:

- Medicaid State Plan Health Homes program data

- Medicaid State Plan Eligibility & Administration program data

- Adult, Child and Health Homes Quality Measure for each Federal Fiscal Year

- User roles and profile

CARTS

The AWS accounts will collect, store, and share the same data previously collected, stored, and shared within the existing AWS account. Other than the AWS account, there will be no changes to how the data is stored nor any new data types.

Statistical Enrollment Data System (SEDS)

This system is complementary to the MDCT CHIP Annual Report Template System (CARTS). SEDS converts an existing paper data collection process into web-based application. It also is designed to

provide the reporting and exporting of survey answers into a PDF template

Managed Care Reporting (MCR)

The application provides state users with the ability to save and submit report data for each of the three MCR reports (MCPAR, MLR, NAAAR). When reported, the gathered information will enable CMCS to better monitor and support state efforts in improving managed care program performance.

Data is not requested or stored that pertains to individuals, rather the data requested and stored pertains to state managed care programs and entities. All information is collected in aggregate.

Quality Measures Reporting (QMR)

MDCT-QMR contains web forms for states input information about their collected data regarding Medicaid and CHIP.

Money Follows the Person (MFP)

The application provides state users with the ability to save and submit report data for each of the MFP reports (WP, SAR). When reported, the gathered information will enable CMCS to better monitor and support state efforts in improving managed care program performance.

Data is not requested or stored that pertains to individuals, rather the data requested and stored pertains to state managed care programs and entities. All information is collected in aggregate.

One Medicaid and CHIP Program System (OneMAC)

The OneMAC system collects First name, Last Name, Company Email while connecting data from States to help CMCS make informed decisions about program oversight.

MC-Review

MC-Review facilitates the review and approval of Medicaid managed care contracts and rate certifications between state agencies and the Centers for Medicare & Medicaid Services (CMS). The system collects, maintains, and shares information to support federal oversight of state Medicaid programs and ensure compliance with regulatory requirements.

Each state user's data (name, email address, state assignments, activity data) is stored distinguish between users and track submission activities for accountability.

Each CMS user's data (name, email address, state assignments, activity data) is stored to distinguish between users, track reviewer actions, and maintain audit trails of federal review decisions.

A state user submits contract and or rate data in a submission(s), then the CMS users can see all this data and perform actions on the submission, such as unlocking, or withdrawing it. Question and answer documents provide a way for the state user and CMS user to send questions and corresponding answers back and forth, without using email.

State contact data is recorded on submissions to allow CMS to message contacts directly for follow-up questions or otherwise discuss

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

Legal Documents

MACPro (Appian)

First / Last name

Email address

Phone number

CMS users Group/Division

CARTS

N/A

Statistical Enrollment Data System (SEDS)

N/A

Managed Care Reporting (MCR)

N/A

Quality Measures Reporting (QMR)

N/A

Money Follows the Person (MFP)

N/A

One Medicaid and CHIP Program System (OneMAC)

First name, Last Name, Company Email

MC-Review

Name, E-Mail Address, Legal Documents

eRegulations (eRegs)

Name and email address for CMCS staff and contractors who log in using CMS IDM Okta. Email address and abbreviated name for contractors who log in with username and password.

Home & Community Based Services (HCBS)

N/A

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

Employees

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

MACPro (Appian)

State Users

CMS Regional Office Users

CMS Central Office Users

CARTS

N/A

Statistical Enrollment Data System (SEDS)

N/A

Managed Care Reporting (MCR)

Employees, Business Partners/Contacts (Federal, state, local agencies)

Quality Measures Reporting (QMR)

N/A

Money Follows the Person (MFP)

N/A

One Medicaid and CHIP Program System (OneMAC)

OneMAC Users (Federal/state/local agencies):

State Users

CMS Regional Office Users

CMS Central Office Users

MC-Review

Employees, Business Partners/Contacts (Federal, state, local agencies)

eRegulations (eRegs)

Employees, Business Partners/Contacts (Federal, state, local agencies)

Home & Community Based Services (HCBS)

N/A

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

MACPro (Appian)

The PII data in MACPro is used for following:

Username to show Point-Of-Contact, User action information on User Interface and System reports

Email address to send notifications

Phone number for Helpdesk to reach out to User

CARTS

N/A

Statistical Enrollment Data System (SEDS)

N/A

Managed Care Reporting (MCR)

N/A

Quality Measures Reporting (QMR)

N/A

Money Follows the Person (MFP)

N/A

One Medicaid and CHIP Program System (OneMAC)

The PII data in OneMAC is used for following:

Username to show Point-Of-Contact, User action information on User Interface and System reports

Email address to send notifications

Also used for user access to the application

MC-Review

Identification for the purpose of tracking the history of actions for audit purposes and accountability for actions completed in the system.

eRegulations (eRegs)

Enable employees and contractors to have user accounts that allow them to view and manage policy-related documents in the application. Enable associating user accounts with changes to documents and metadata for audit logging purposes.

Home & Community Based Services (HCBS)

N/A

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

Not Applicable. There is no other secondary use of PII.

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

Title 5 (TITLE 5—GOVERNMENT ORGANIZATION AND EMPLOYEES) USC 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.

Directly from an individual about whom the information pertains

Online

Government Sources

Identify the OMB information collection approval number and expiration date

State OMB Control Number: 0938-1188

Expiration Date: 07/31/2027

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.

MACPro (Appian)

During the first attempt to register and every time that user accesses the CMS Identity Management System (IDM) and MACPro the user must agree to the Terms & Conditions of the usage. As part of the User Terms & Conditions, it is mentioned that the user should not have any reasonable expectation of privacy regarding any communication or data transiting or stored on these systems. The user data will be monitored, intercepted, searched and seized any communication or data transiting or stored on this system at any time and for any lawful Government purpose. The notification process occurs at the IDM new user registration screen and then subsequently at the user access screen of IDM.

CARTS

N/A. PII is not collected.

Statistical Enrollment Data System (SEDS)

N/A, PII is not collected.

Managed Care Reporting (MCR)

N/A. PII is not collected.

Quality Measures Reporting (QMR)

N/A. PII is not collected.

Money Follows the Person (MFP)

N/A. PII is not collected.

One Medicaid and CHIP Program System (OneMAC)

During the first attempt to register and every time that user accesses the CMS Identity Management System (IDM) and OneMAC the user must agree to the Terms & Conditions of the usage. As part of the User Terms & Conditions, it is mentioned that the user should not have any reasonable expectation of privacy regarding any communication or data transiting or stored on these systems. The user data will be monitored, intercepted, searched and seized any communication or data transiting or stored on this system at any time and for any lawful Government purpose. The notification process occurs at the IDM new user registration screen and then subsequently at the user access screen of IDM.

MC-Review

The application's notification is carried out by the IDM login system itself. Login is completed via IDM, which requires users to accept the Terms & Conditions, which state clearly that information will be recorded and that there is no reasonable expectation of privacy when using the system.

eRegulations (eRegs)

This is done via CMS IDM Okta.

Home & Community Based Services (HCBS)

N/A. PII is not 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.

MACPro (Appian)

The ability to opt-out of the collection of PII is handled at the CMS IDM Okta level. Any individual seeking access must first have an IDM account. The users must accept the Terms & Conditions before accessing the MACPro application. The Terms & Conditions advises the user that they are accessing a U.S. Government system and there should be no reasonable expectation of privacy.

CARTS

N/A. PII is not collected directly from users. Access is handled via CMS IDM Okta. Users may choose to request access to applications via IDM roles or decline if they don't want to provide their information/contacts to the application.

Statistical Enrollment Data System (SEDS)

N/A. PII is not collected directly from users. Access is handled via CMS EUA. Requesting a job code for the application and using the application are both optional.

Managed Care Reporting (MCR)

N/A. PII is not collected directly from users. Access is handled via CMS IDM Okta. Users may choose to request access to applications via IDM roles or decline if they don't want to provide their information/contacts to the application.

Quality Measures Reporting (QMR)

N/A. PII is not collected directly from users. Access is handled via CMS IDM Okta. Users may choose to request access to applications via IDM roles or decline if they don't want to provide their information/contacts to the application.

Money Follows the Person (MFP)

N/A. PII is not collected directly from users. Access is handled via CMS IDM Okta. Users may choose to request access to applications via IDM roles or decline if they don't want to provide their information/contacts to the application.

One Medicaid and CHIP Program System (OneMAC)

N/A. PII is not collected directly from users. Access is handled via CMS IDM Okta. Users may choose to request access to applications via IDM roles or decline if they don't want to provide their information/contacts to the application.

MC-Review

PII is not collected directly from users. Access is managed through CMS IDM Okta. Users may opt out by declining to provide their email address; however, an email address is required to enable

system generated notifications and to allow CMS users to contact state users associated with a submission under review.

eRegulations (eRegs)

PII is not collected directly from users. Requesting a job code for the application and using the application are both optional.

Home & Community Based Services (HCBS)

N/A. PII is not collected directly from users. Access is handled via CMS IDM Okta. Users may choose to request access to applications via IDM roles or decline if they don't want to provide their information/contacts to the application.

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

The ability to opt out of the collection of PII is managed at the CMS IDM Okta level. Any individual seeking access to the application must first establish an IDM account. When a user submits a job code or IDM role request to obtain access, their user details and contact information are transmitted to the application through IDM/EUA. This contact information is used to notify system users of major changes to the system, including changes to disclosures or data uses. Consent to collect and use PII is obtained as part of the IDM account creation and access request process.

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.

Individuals who believe their PII has been inappropriately obtained, used, disclosed, or is inaccurate may contact the CMS IDM/EUA Help Desk by phone or email to report their concerns. The CMS IDM/EUA Help Desk documents the issue, investigates the concern in accordance with CMS policies and procedures, and coordinates with appropriate system owners or security personnel as needed to resolve the issue and help the individual.

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

Periodic reviews of PII contained in the system are conducted to ensure data integrity, availability, accuracy, and relevancy. User PII is sourced from CMS IDM Okta/EUA and is reviewed as part of routine access management activities, including role validation, access recertification, and account maintenance. System administrators and authorized CMS personnel monitor user access and associated PII to ensure it remains accurate and relevant to the user's role. Inactive or outdated accounts are reviewed and deactivated in accordance with CMS policies, and any identified discrepancies are addressed promptly to maintain data quality and integrity.

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

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

PII is not collected directly from users. Access is handled via CMS IDM Okta. System users, including administrators, developers, and contractors, are granted access based on role-based access controls and the principle of least privilege. Users must have a validated business need for access, and access requests are approved through the IDM/EUA process by authorized CMS officials. User roles and permissions determine the level of PII access granted. Access is reviewed periodically during access recertification and account maintenance, and permissions are modified or

revoked promptly when no longer required.

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.

Access to PII is controlled through role-based access controls and the principle of least privilege. Users, administrators, and contractors are granted only the minimum level of access necessary to perform their job functions. System permissions are assigned based on approved roles in CMS IDM/Okta role and EUA job code. Access is regularly reviewed through access recertification processes

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.

Personnel using the system, including system owners, managers, operators, contractors, and program managers, are provided with comprehensive role-based training to ensure awareness of their responsibilities for protecting information collected and maintained by the system. Training addresses management, operational, and technical roles and responsibilities and covers physical, personnel, and technical safeguards and countermeasures. In addition, users are required to complete CMS privacy and security awareness training on an annual basis as a condition of continued system access.

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

Personnel using the system, including system owners, managers, operators, contractors, and program managers, are provided with comprehensive role-based training to ensure awareness of their responsibilities for protecting information collected and maintained by the system. Training addresses management, operational, and technical roles and responsibilities and covers physical, personnel, and technical safeguards and countermeasures. In addition, users are required to complete CMS privacy and security awareness training on an annual basis as a condition of continued system access.

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 destroying "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.

PII in the system is protected through a combination of administrative, technical, and physical controls. Administrative controls include CMS policies and procedures, role-based access approvals through CMS IDM Okta, annual privacy and security training requirements, and periodic access reviews. Technical controls include role-based access controls, authentication via IDM Okta, encryption of data in transit and at rest, audit logging, and system monitoring to detect unauthorized access or activity. Physical controls include CMS-approved data center protections, such as facility access controls, surveillance, and environmental safeguards, which prevent unauthorized physical access to system infrastructure.

Identify the publicly-available URL:

MACPro (Appian)

<https://macpro.cms.gov/>

CARTS

<https://mdctcarts.cms.gov>

Statistical Enrollment Data System (SEDS)

<https://mdctseeds.cms.gov>

Managed Care Reporting (MCR)

<https://mdctmcr.cms.gov/>

Quality Measures Reporting (QMR)

<https://mdctqmr.cms.gov/>

Money Follows the Person (MFP)

<https://mdctmfp.cms.gov/>

One Medicaid and CHIP Program System (OneMAC)

<https://onemac.cms.gov>

MC-Review

<https://mc-review.onemac.cms.gov>

eRegulations (eRegs)

N/A – Internal to CMS only

Home & Community Based Services (HCBS)

<https://mdcthcbs.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?

No

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