US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/21/2026

OPDIV:

CMS

Name:

Marketplace Lite

PIA Unique Identifier:

P-9175612-272177

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

Significant System Management Change

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

Marketplace lite is implementing new front-end user interface (UI) component as part of the Marketplace Eligibility Application (MEA) which is included in the Marketplace Lite (MPL) application. The change includes connections to systems outside of the Marketplace Lite authorization boundary. The new connection is to the CMS Federal Information Security Modernization Act (FISMA) system Document Storage and Retrieval Service (DSRS). This change introduces a new Application Programming Interface (API) call to an approved existing external system, Standalone Eligibility Services (SES). The new API call to the Get Eligibility Results endpoint includes transfer of new Personally Identifiable Information and Protected Health Information.

Describe the purpose of the system.

The Center for Medicare & Medicaid Services (CMS) Office of Communications (OC) designed Marketplace Lite (MPL) to provide an easy-to-use application process for individuals to enroll in

health insurance coverage on the Federally Facilitated Marketplaces (FFM) website, healthcare.gov. FFM is covered by its own Privacy Impact Assessment (PIA).

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

The Marketplace (MPL) application process collects, maintains, and shares the following categories of information:

Personal Identifying Information: First, Middle, and Last Names; Suffix; Email Address; Home Address; Phone Number; Social Security Number; Pregnancy Information; Federally Recognized Tribe Membership; Relationships; Veteran Status; Foster Care Information; Citizenship Information; and Dependent Information and Relationships.

Employment and Income: Employment Information; Annual Income; and Employer Name.
Language and Demographics: Ethnicity; Race; Sex Assigned at Birth; Sexual Orientation; Spoken Language; and Written Language.

Coverage and Assistance: Current Health Care Coverage; Coverage State; Policy Assistor Name and Suffix; Medicare Coverage Dates; Medicaid Program Information; Member Enrollments and Coverage Records; Premium Amounts and Coverage Dates; Advance Premium Tax Credit (APTC) Records and Amounts; Special Enrollment Period (SEP) Types; Coverage Year; Insurance Application Identifier; Application Status; Submission Origin Type; and Last Consumer Submission Date and Time.

Member-Level Information: Person Tracking Number; Qualified Health Plan (QHP) Status and Reason; Advance Premium Tax Credit (APTC) Status and Reason; Secretary Hardship Indicator; Cost-Sharing Reduction (CSR) Status and Reason; Cost-Sharing Reduction (CSR) Variant; Medicaid Status and Reason; Children's Health Insurance Program (CHIP) Status and Reason; Emergency Medicaid Status and Reason; Unborn Child Children's Health Insurance Program (CHIP) Status and Reason; Transfer Applicant to State Status and Reason; and Medicaid Non-Modified Adjusted Gross Income (Non-MAGI) Referral Status and Reason.

Health Reimbursement Arrangement (HRA) and Employer Coverage: Health Reimbursement Arrangement (HRA) Event; Individual Coverage Health Reimbursement Arrangement (ICHRA) Result Status and Reason; Health Reimbursement Arrangement (HRA) Offers; Employer Name; Health Reimbursement Arrangement (HRA) Type; Primary Insured Member Identifier; Safe Harbor Indicator; and Health Reimbursement Arrangement (HRA) Affordability Indicator.

Tax Household Information: Tax Households; Tax Household Status and Reason; Tax Household Member Identifier; and Maximum Advance Premium Tax Credit (APTC).

Special Enrollment Period (SEP) Details: Special Enrollment Period (SEP) Status and Reason; Start and End Dates; Special Enrollment Period (SEP) Type; and Associated Member Identifiers.
Submission Metadata and Attestations: Coverage State; User Identifier; Linked System User Identifier; Attestations; Contact Member Identifier; Contact Method; Email (Primary and Secondary); Mobile Phone; Spoken Language; and Written Language.

Member Demographics and Coverage: First, Middle, and Last Name; Suffix; Insurance Coverage; Health Reimbursement Arrangement (HRA) Offers and Types; Coverage Start and End Dates; and Medicare Start Date.

Verification Issues: Identifier; Creation Date and Time; Issue Type and Sub-Type; Status Type; End Date; Category; and Special Enrollment Period (SEP) Issue Status Type.
Notices and Documentation: Document Storage and Retrieval System (DSRS) Identifier; Document

Subcategory; and Document Creation Date and Time.

Reference Data: Medicaid and Children's Health Insurance Program (CHIP) Program Names and Phone Numbers; Teletypewriter (TTY) Phone Numbers; Eligibility Indicators; Open Enrollment and Special Enrollment Period (SEP) Cutoff Dates; and Bar Opt-Out Information.

Enrollments and Policies: Insurance Application Identifier; Exchange Policy Identifier; Issuer Health Insurance Oversight System (HIOS) Identifier and Name; Insurance Plan Identifier and Name; Plan Metal Level Type; Essential Health Benefits (EHB) Premium Amount; Cost-Sharing Reduction (CSR) Variant and Amounts; Policy Member Coverage, Premium, and Relationship Records; and Assistor Records including National Provider Number, Name, and Start and End Dates.

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

MPL is the application process used through HealthCare.gov to support consumers in creating accounts, submitting applications, and receiving eligibility determinations for Marketplace coverage and related financial assistance programs. MPL does not retrieve consumer or household member records using personal identifiers such as name, Social Security Number (SSN), date of birth, or address. All records are retrieved exclusively through system-generated identifiers, including application IDs, account IDs, and internal tracking numbers. This retrieval method applies to all categories of individuals, including applicants, dependents, identity-verification participants, and system administrators.

1. Consumers Creating an Account or Applying for Coverage
Information Collected: Full name; date of birth; address; email; phone number; SSN; citizenship/immigration status; pregnancy information; Tribal membership; veteran status; foster care information; relationship information; employment information; annual income; current health coverage; sexual orientation; sex assigned at birth; ethnicity; race; preferred spoken/written language.
Purpose: Supports account creation, identity verification, and eligibility determinations for Qualified Health Plans (QHPs), Advance Premium Tax Credits (APTC), Cost-Sharing Reductions (CSR), Medicaid, and CHIP. Ensures accurate household composition and income assessment.
Retrieval Method: Not retrieved by PII. Records are retrieved using system-generated identifiers (e.g., application ID, account ID).

2. Household Members (Dependents)
Information Collected: Name; date of birth; relationship to applicant; SSN (if provided); citizenship information; pregnancy status; Tribal membership; veteran status; foster care information; income and coverage information (if applicable).
Purpose: Required to determine eligibility for Marketplace coverage, APTC/CSR, Medicaid, and CHIP at the household level.
Retrieval Method: Not retrieved by PII. Records are retrieved using internal identifiers linked to the primary application.

3. System Users and Administrators
Information Collected: User ID; password; role-based access information.
Purpose: Used to authenticate authorized personnel supporting MPL operations, maintenance, and troubleshooting.
Retrieval Method: Not retrieved by PII. Administrative records and access logs are retrieved using system-assigned user identifiers.

4. Consumers Providing Coverage or Program Participation Information
Information Collected: Medicare coverage dates; Medicaid/CHIP status and reasons; Emergency

Medicaid status; Unborn Child CHIP status; HRA/ICHRA information; QHP status; APTC/CSR determinations; Special Enrollment Period (SEP) types and dates.
Purpose: Supports eligibility determinations for Marketplace programs, financial assistance, and SEP qualification; enables coordination with federal and state health programs.
Retrieval Method: Not retrieved by PII. Records are retrieved using system-generated identifiers.

5. Consumers Providing Documentation or Verification Responses
Information Collected: Verification issue identifiers; creation dates; issue types; status types; notices; Document Storage and Retrieval System (DSRS) identifiers.
Purpose: Supports resolution of eligibility verification issues, compliance with federal verification requirements, and documentation for program integrity.
Retrieval Method: Not retrieved by PII. Verification records are retrieved using issue identifiers or application IDs.

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
Phone Numbers
Financial Accounts Info
Employment Status
Other: Pregnancy Information Federally Recognized Tribe Membership Relationships, Veteran Status, Foster Care Information, Citizenship Information, Dependent Information and Relationships, Employment Information, Annual Income, Current Healthcare Coverage, Ethnicity (Optional), Race (Optional), Sex- Assigned at Birth, Sexual Orientation, Spoken Language, Written Language, Coverage State, Policy Assistor Name; First Name Last Name Middle Name Suffix Employer Name Medicare Coverage Dates Medicaid Program Information Member Enrollments and Coverage Records Premium Amounts and Coverage Dates Tax Credit Records and Amounts Special Enrollment Period Types (Life Events)

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

Employees
Public Citizens
Vendor/Suppliers/Contractors
Health insurance agents and brokers

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is collected and used to validate an individual's identity and eligibility determination for enrollment in a Qualified Health Plan. For system support personnel, it is used to access the system.

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

This is not applicable to MPL.

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

ACA 42 U.S.C. sections 1411(c),1411(d) and 1414; 18031, 18041, 18081—18083

45 CFR 155.200

5 U.S.C. 301, Departmental Regulations

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

No

09-70-0560, Modification to the Health Insurance Exchange (HIX) SORN, October 23, 2013

09-70-0560, Health Insurance Exchanges (HIX) Program SOR, May 27, 2013

09-70-0560, Health Insurance Exchanges (HIX) Program, 2/6/2013 and updated 5/29/2013 and

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB Control Number: 0938-1156

Title: Establishment of Qualified Health Plans and American Health Benefit Exchanges (CMS-10400)

Expiration Date: 09/30/2027

OMB Control Number: 0938-1191

Title: Data Collection to Support Eligibility Determinations for Insurance Affordability Programs and Enrollment through Health Benefits Exchanges, Medicaid, and Children's Health Insurance Program Agencies

Expiration Date: 09/30/2027

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.

As part of the application process and creating an online account, an individual is presented with the Healthcare.gov Privacy Policy and must click a checkbox to acknowledge that they understand it. There is a link to the Privacy Policy at each stage of the application process, which also includes a Privacy Act Statement.

If an individual elects to apply by mail or online, the Marketplace Application form has a privacy notice on it that has been updated.

Users who register by phone or in person are also notified that their personal information will be collected for registration purposes.

For individuals who apply using a paper-based Marketplace Application, the form includes a clearly displayed privacy notice and Privacy Act Statement before any fields requesting personal information. This ensures applicants understand the purpose, authority, and use of their information prior to completing or submitting the form.

Across all channels—online, paper, phone, and in-person - MPL provides prior notice consistent with Privacy Act requirements, and no personal information is collected without informing individuals of the purpose, authority, and intended use of the information.

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 option for consumers to opt-out of providing PII, since it is necessary to register for health insurance. It is also necessary that the system collect PII of system support staff for identification and authentication as well as tracking/auditing purposes.

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

Since MPL is part of the Federally-facilitated Marketplace (FFM) and operates through HealthCare.gov, MPL follows the FFM's established process for notifying individuals of major system changes. When significant updates occur that affect how personal information is collected, used, maintained, or shared, the FFM posts updated notices, policies, and Privacy Act Statements directly on HealthCare.gov. This serves as the primary public-facing mechanism for informing individuals of changes to data practices.

Also, when the Marketplace updates its data practices, the paper application form is revised accordingly, and the updated notice is provided to all individuals who apply using the paper form going forward. This ensures that paper-based applicants receive the most current privacy information at the time of collection, consistent with Privacy Act requirements.

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 have concerns about their PII can contact the Health Insurance Marketplace call center at 1-800-318-2596.

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

CMS has a National Institute of Standards and Technology (NIST)-compliant continuous monitoring program with regularly scheduled system audits, at least annually, and monthly/quarterly scanning to ensure system integrity and availability. As part of CMS, MPL is included within that monitoring system.

To ensure the integrity, availability, accuracy, and relevancy of the PII in MPL, the following methodologies are used. MPL users can manage their own PII by editing their profile after they have registered with the system for data integrity, accuracy and relevancy. MPL does a cross-check with FFM for data integrity and account management purposes. MPL is designed with encryption and role-based access controls to ensure data accuracy, and integrity. Encryption is applied to data in transit and data at rest.

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.

The MPL user interfaces limit the display of PII to only those elements needed to perform specific tasks. Role-based access controls ensure system support staff are granted access on a "need-to-know" and "need-to-access" basis which correspond to their assigned duties. The CMS System Owner determines who has an administrative account on this system and reviews all accounts periodically and as needed.

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.

There are three methods for restricting access. First, is to program user interfaces to limit the display of sensitive information, such as Personally Identifiable Information (PII) to only those elements needed to perform specific tasks. Second, PII is only transmitted to validate information rather than copy or pull information from another source. Third, role-based access controls and auditing ensure those with access have a "need-to-know" and "need to access".

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.

Both CMS employees and contractor staff who access or operate MPL are required to complete the annual CMS Security Awareness training provided annually as computer based training (CBT) course. Contractors also complete their annual corporate security training.

Individuals with privileged access must also complete role-based security training commensurate with the position they are working in.

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

Not applicable.

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.

MPL follows the CMS Records Schedule that was published in April 2015 and the National Archives and Records Administration General Records Schedule (GRS) 5.1 and 5.2 (July 2017).

Specifically, for PII that is securely stored in the MPL database, the National Archives Records Association (NARA), General Records Schedule (GRS) 5.1 states that MPL will destroy such record immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use. GRS 5.2 states that MPL will destroy records upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

NARA Schedule: DAA-GRS2016-00160002
DAA-GRS2022-00090002

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

Administrative Controls
- Mandatory security and privacy training for all users with access to MPL
- Enforcement of “need-to-know” and “minimum necessary” principles when granting access
- Role-based access controls and periodic access reviews
- Documented policies and procedures governing proper handling of PII
- Incident response processes and continuous monitoring of compliance

Technical Controls
- Firewalls, intrusion detection and prevention systems, and continuous network monitoring
- Multi-factor authentication for system access
- Encryption of data in transit and at rest
- Audit logging and automated alerts for anomalous activity
- Secure configuration baselines and vulnerability management

Physical Controls
- System servers housed in secure data centers with guard services, locked access points, and surveillance
- Environmental protections such as climate control, fire suppression, and redundant power
- Restricted physical access to authorized personnel only

Identify the publicly-available URL:

http://www.healthcare.gov/app

http://www.cuidadodesalud.gov/app

These are still legit URLs. You may clear cache, if needed

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.

Other technologies that do not collect PII:

Measurement tools are used to monitor website traffic: frequency and repeated visits and busy (peak) periods.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

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

Yes