US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/25/2026

OPDIV:

CMS

Name:

CMS Enterprise Portal Services

PIA Unique Identifier:

P-9568808-529482

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?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Internal Flow or Collection

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

No changes since the last PIA.

Describe the purpose of the system.

The Centers for Medicare and Medicaid Services developed the Enterprise Portal Services which is a single interface for this agency user community to access applications hosting this agencies data. The portal provides an enterprise-wide secure gateway to the end-users through Web applications, portlets, and Business Intelligence reports which help with visualization of the data present in this agency data repository. The portal has the capability to perform the following functions:

Provides a Single Sign On mechanism to integrated applications.

Provides security, cache controls, and other traffic management features through Akamai.

Integrates portlets or applications/tools, provided by application teams, with the portal services. These tools may include Commercial off-the-Shelf tools or custom software.

Provides collaboration services using International Business Machines Corporation.

Provides content management using Web Content Management services.

Provides an understanding of the unique number of visitors, the pages the visitors clicked, and how much time they spent on those pages using Chartbeat and New Relic.

Provides self-service operations such as new user registration.

Provides an Enterprise Portal Object Repository service to enable users to upload and download files.

Provides a Portal Self-Service Console which serves as a centralized access hub that allows users to launch, subscribe to, and learn more about the available Enterprise Portal Self-Service tools.

Provides an Enterprise Portal Object Repository Self-Service tool to allow vertical applications with the ability to perform most of the administrative functions involved in integrating with the portal shared service.

Provides a “chat-as-a-service” (Chatbot) feature to guide end users and help people solve problems or get answers to questions without having to call the help desk or wasting time on searching and browsing through the documentation, web sites, and/or applications.

The goal is to eliminate the multiple points of entry, user identifiers, and paths while providing an opportunity for central communication and offering the user a better experience with accessing the Centers for Medicare and Medicaid Services applications.

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

The Enterprise Portal Services is a gateway for the Centers for Medicare and Medicare Services systems that collects and maintains the username and user password for the duration of the user account being active. The user consists of this agency's personnel, contractors and Business Partners.

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

The Enterprise Portal Services collects and maintains the username and user password.

The Enterprise Portal Services maintains the information for the duration of the user account being active. The user consists of this agency's personnel, contractors and Business Partners.

Upon login, the username and user password are needed for the end user to register and to access this agency's systems.

Note: Personal identifiers are not used to retrieve any records held in the system.

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

Yes

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

User name; User password

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

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The system collects Personal Identifiable Information to provide a means of identifying the authorized users who are accessing applications through the Portal.

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.

U.S.C. § 7701(c)(1), Appellate procedures

5 U.S.C. Section 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
In-Person
Email
Online
Government Sources
Within OpDiv
Non-Government Sources
Private Sector
Other

Identify the OMB information collection approval number and expiration date

OMB: 0938-1236 Expiration: 08/31/2025

The CMS Identity Management System (CMS-10452)

The OMB control number will not change, but it is not currently valid. It will be reinstated at the conclusion of the resubmission process (approx. 9 months after OIT submits the completed package to OSORA). The expiration date will be updated once OMB concludes its review and formally reapproves the package.

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.

When users provide the Portal system with their login credentials, they are presented with a login banner. This login banner states that Portal will collect users' Personal Identifiable Information to verify their identity.

By continuing to use Portal, users implicitly consent to have their Personal Identifiable Information collected.

In addition, the Centers for Medicare and Medicaid Services Website Privacy Policy can be accessed from any page on this agency's website. This policy provides users with an explanation of how this agency collects and uses their information when individuals access this agency's resources online. https://www.cms.gov/privacy/index#h54sjsyz19p0bxvl76ovmlft1x1hhm5

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 the user to object to the collection of their Personal Identifiable Information. Providing a username and password is required to access the system. If a user chooses not to accept the terms and Conditions during the initial registration, then a user account cannot be created for the user. Therefore, the user will not be able to access the agency applications that require login credentials.

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

Portal does not notify users when a change occurs in the system.

Access to Portal is managed through Centers for Medicare and Medicaid Services' Enterprise User Administration system. Enterprise User Administration is a web-based application that manages access to many of this agency's systems.

Please note that all systems named here are covered under their own Authority to Operate and Privacy Impact Assessments.

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 has a concern or a question regarding his or her PII, then he or she may contact the Centers for Medicare and Medicaid Services' Privacy Office by telephone at (410)-786-5357 or by email at privacy@cms.hhs.gov.

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

Personal Identifiable Information exists within the Enterprise Portal System boundary. Since access to portal is managed through the Enterprise User Administration, the methods for ensuring the integrity, availability, accuracy, and relevancy of the system's PII are maintained within the Enterprise User Administration system. Portal relies on automatic updates from the Enterprise User Administration regarding users' access to Personal Identifiable Information. Portal doesn't perform reviews on this Personal Identifiable Information because it is the responsibility of Enterprise User Administration. Firewalls and encryption ensure the integrity of the system information.

User credentials are reviewed by Enterprise User Administration at least annually and access verified and adjusted as necessary,

Please note that all systems named here are covered under its own Authority to Operate and Privacy Impact Assessment.

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.

Access to Portal Personal Identifiable Information is managed through the Enterprise User Administration system. Before this agency employee (s) or contractor (s) and/or vendor can obtain access to Personal Identifiable Information related to the Portal system, a request must be formally submitted. This access is granted only upon approval from Enterprise User Administration Access Authorizer.

Please note that all systems named here are covered under its own Authority to Operate and Privacy Impact Assessment.

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.

The method that Portal uses to allow minimal access to Personal Identifiable Information is the principle of "least privilege." The only individuals who can access Personal Identifiable Information are those who have a "need to know" to complete their job responsibilities. This is determined according to everyone's business role. Access is managed by this agency's Enterprise User Administration system, and it is only granted following a formal request.

Please note that all systems named here are covered under its own Authority to Operate and Privacy Impact Assessment.

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 of this agency's personnel and direct contractors are required to take the Centers for Medicare and Medicaid Services Security and Privacy Awareness training annually or whenever changes to the training module are made. This training includes details on the handling of Personal Identifiable Information.

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.

Records will be held indefinitely until no longer needed for agency use. Portal follows the retention schedules of:

National Archives and Records Administration GENERAL RECORDS SCHEDULE 3.2: Information Systems Security Records item 30 (August 2015)

National Archives and Records Administration GENERAL RECORDS SCHEDULE 4.3: Input Records, Output Records, and Electronic Copies, item 31 (August 2015)

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

Portal utilizes administrative, technical, and physical controls to secure Personal Identifiable Information.

Administrative controls include security and network policies and procedures as well as user access procedures.

Technical security controls include the encryption of data in transmission, the use of firewalls, and the use of antivirus software. Portal also uses intrusion detection/prevention technologies.

The physical controls include having the server and data storage environment within a secure, access-controlled data center. This data center provides 24-hour security and video monitoring.

Session Cookies - Collects PII?: Yes
Note: web address is a hyperlink.