US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/20/2025

OPDIV:

CMS

Name:

Eligibility Appeals Case Management System

PIA Unique Identifier:

P-2474134-594075

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

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

None

Describe the purpose of the system.

As a result of the 2010 Affordable Care Act, the Department of Health and Human Services (HHS) was tasked to implement the Federally Facilitated Marketplace (FFM) Exchanges, covered by its own Privacy Impact Assessment (PIA). As part of the Federal Health Exchange system, the Eligibility Appeals Case Management Systems (EACMS) was established as the system of record for the Eligibility Appeals process for those people who are appealing eligibility decisions to participate in the FFM. EACMS provides case management functions and stores all Eligibility Case information, provides workflows at every stage of the Eligibility Case, and supports the Federally Facilitated Marketplace (FFM) Eligibility Appeals Support (FEAS) system, covered by its own PIA.

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

Citizenship, Immigration Status, Veteran Status, Employment Status, Current and Annual Projected Modified Adjusted Gross Income (MAGI), Incarceration Status, Indian Status, Employer Sponsored Minimum Essential Coverage (ESC MEC), Non-Employer Sponsored Minimum Essential Coverage (Non-ESC MEC), Residency, Social Security Number (SSN), Hardship Exemption, Incarceration Status Exemption, Indian Health Services Exemption, Religious Conscience Exemption, Identity (Name, Driver's License, Passport, Date of Birth, Mailing Address, Email Address, Phone Number, Taxpayer ID), Name Change, Medical Notes, Legal Documents, Photographic Identifiers, Financial Account Info. Also, login credentials, user ID, and password are used for access into the system. The submission of personal information is required to substantiate the appeal process.

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

EACMS uses the PII listed for the reasons below. The PII is maintained for the duration of the appeals process.

EACMS uses the PII to initiate appeals, provide systemic informal resolution and pre-hearing support, provide federal hearing officers with case data during appeal hearings for review and update, and provide data tracking of appeal caseloads, including the reporting of the close-out of appeals. The types of appeals are described below:

Specifically, for Individual Eligibility Appeals, PII is used for eligibility for advanced payments of the premium tax credit, cost sharing reductions, Medicaid, Children's Health Insurance Program (CHIP), enrollment in a Qualified Health Plan (QHP), and eligibility for an enrollment period, including Special Enrollment Period (SEP), and for the catastrophic coverage provision. Additionally, the failure of an Exchange to provide timely notice is appealable.

Additionally, for Individual Eligibility Appeals, PII is used for eligibility for an exemption from the individual responsibility requirement. Specifically, for Employer appeals, PII is used for appeals from a notice that the employer may be liable for a tax penalty because it has failed to provide affordable, minimum essential coverage to its employees. PII is also used for eligibility for the Small Business Health Options Program (SHOP) Exchange, including both employee and employer eligibility.

Appeals records can be retrieved by any PII data element provided to the system by hearing support staff and federal hearing officers.

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
Photographic Identifiers
Driver's License Number
E-Mail Address
Mailing Address
Phone Numbers
Medical Notes
Financial Accounts Info
Legal Documents
Employment Status
Passport Number
Taxpayer ID

Login Credentials, Citizenship, Immigration Status, Veteran Status, Current and Annual Projected Modified Adjusted Gross Income (MAGI), Incarceration Status, Indian Status, Employer Sponsored Minimum Essential Coverage (ESC MEC), Non-Employer Sponsored Minimum Essential Coverage (Non-ESC MEC), Residency, Hardship Exemption, Incarceration Status Exemption, Indian Status /Indian Health Services Exemption, Religious Conscience Exemption, Identity, Name Change

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

Employees
Public Citizens
Vendor/Suppliers/Contractors
Employers, Appellants

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of PII in the EACMS is for the eligibility appeals process. The system also uses PII, in the form of employee login credentials, to provide access to the system.

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

None

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

Patient Protection and Affordable Care Act (PPACA) (Pub. L. 111–148) as amended by the Health Care and Education Reconciliation Act of 2010 (Pub. L. 111–152), collectively referred to as the Affordable Care Act.

45 Code of Federal Regulations (CFR) 155.500, 155.700, 155.20, 155.305,

Federal tax return information can only be used or disclosed as authorized by 26 U.S.C. 6103

Title 42 U.S.C. 18031, 18041, 18081, 18083, and sections 2723, 2761 of the Public Health Service Act (PHS Act), and E.O. 9397.

5 U.S.C. 301 Departmental 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.

09-70-0560 Health Insurance Exchanges (HIX) 10/23/2013

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Hardcopy
Email
Government Sources

Identify the OMB information collection approval number and expiration date

0938-1207 expired 6/30/2025, an updated expiration date for OMB Control Number 0938-1207 is

Within OpDiv

Non-Governmental Sources

Public

Private Sector

not available. The ICR associated with the subject OMB control number is still in the middle of the resubmission process. Specifically, it is nearing the end of its 60-day FR notice and comment period. The comment period ends July 21, 2025. Once the comment period ends and, if applicable, CCIIO reconciles any public comments received, we will publish a second FR notice with a 30-day public comment period. At that point, the ICR will be formally submitted to OMB. OMB approval is not likely until mid-Fall 2025, at the earliest.

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.

Privacy notices are provided to the appellant in both the Appeal Request Form and the Appeal Acknowledgement Letter. Both are provided to the Appellant by the Federally Facilitated Marketplace and not by EACMS. These privacy notices inform the appellant that FFM protects the information collected during the Eligibility Appeal process.

For Employees, Login Banner Statements are displayed and must be agreed upon prior to access to the EACMS Application. The login banner states that employees' actions are monitored while accessing EACMS.

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.

EACMS does not allow opt-out of collections or use of PII. To appeal an eligibility decision, the potential appellant is required to provide PII for verification purposes to the Health Insurance Marketplace.

For employees, the banner statement must be agreed upon prior to gaining access to EACMS.

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

PII stored in EACMS is collected by FFM as part of the appeals process, please refer to the FFM PIA for the notification process.

Employee PII: employees are notified by the MAXIMUS Federal of all major changes prior to deployment via email if Login Credential PII is affected. Employees are required to re-accept the Login Banner prior to accessing the system after the change is completed.

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.

Appellants follow the notification process by writing a letter to Health Insurance Marketplace.

Appellants can also contact the Eligibility Appeals Operation Support (EAOS) Center Help Line.

Employees and contractors can contact the EACMS Operations Team or the EAOS Center Help Line to resolve PII concerns.

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

Integrity: Federally Facilitated Marketplaces (FFM) Eligibility Appeals Support (FEAS) system

performs periodic reviews of PII stored in EACMS. These processes include manual review of exchange data extracts. Incoming hard copy appeals for information are reviewed daily for discrepancies. All appeals discrepancies are reviewed and documented.

Accuracy: All documented appellant discrepancies are updated in EACMS by the EACMS Appeals Team. For Employees, all discrepancies are documented and updated by the EACMS Operations Team.

Availability: EACMS is expected to be available 24/7. Because of this, data matching technologies are in use to both review accuracy and availability of Eligibility Appeal Data.

Relevancy: Federally Facilitated Marketplaces (FFM) Eligibility Appeals Support (FEAS) system performs periodic quality assurance reviews of the PII contained in EACMS, please refer to the FEAS PIA.

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 PII information by system users is determined by utilizing role-based access based on Least Privileges. EACMS has created the following roles:

System Administrators containing full access to the systems to which they are assigned for system maintenance and support.

Application Administrators have limited access to the operating system functions, but full access to assigned application components for application maintenance enhancement and future releases.

Security auditors and analysts have access to auditing and security monitoring for security control audits and reporting in addition to monitoring environmental activity.

These roles are given least privileges to perform their duties and will have to request approval before being granted escalated privileges.

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.

Users are granted a specific level of access to the operating system on which they are working. This access is only granted after an approval process is performed via the ticket management system. After approval, access is granted for specific named role access to a system. Users with certain access can only perform specific actions on that system, such as WebSphere Application Server (WAS) administrators cannot perform administrator functions on a Unix system.

Each role has the minimum privilege needed to accomplish the assigned work. Users are assigned role-based on the concept of least privileges. Administrator roles are granted so that they can perform only the tasks which they need to while blocking them out from all other tasks. Employees must be authorized by their manager as well as the System Security Officer to perform privileged functions. Active Directory is used to enforce the least privilege in conjunction with our ticketing system and audit log reviews for escalated privileges.

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.

EACMS program contractors institute a Security Awareness and Training (SAT) program providing all government programs personnel with general security awareness training upon hire (before accessing EACMS systems) and annual refresher training thereafter. In addition, there are periodic reminders via e-mail, workplace posters, etc.

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

The System Security Officer (SSO) is responsible for ensuring that all personnel are appropriately trained and have signed a Security Awareness and Training (SAT) acknowledgement and agreement forms. User training consists of a one-hour briefing emphasizing security awareness and policies in addition to fire and safety training. The curriculum includes the purpose of security, security contacts, the Health Insurance Portability and Accountability Act (HIPAA), IRS and privacy awareness, types of malicious activities, recognition of security incidents and the requirement to report them. Rules of Behavior, such as securing sensitive information, securing workstations, using licensed software, prohibitions against network or workstation modification, incident reporting, and password management are covered in Security Awareness Training. In addition, building and physical security guidelines are stressed, and staff are encouraged to report safety issues. Corporate Code of Conduct training is given annually via web training Learning Management System (LMS). This training, which overlaps SAT, details corporate policies and procedures and how they apply to each employee. Reports are generated by the LMS. The Training department ensures that everyone takes the training and agrees to it annually.

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.

EACMS data will be maintained for a period of up to 10 years after entry in the database. Any such records that are needed longer, such as to resolve appeals and audit exceptions or to prosecute fraud, will be retained until such matters are resolved. Beneficiary claims records are currently subject to a document preservation order and will be preserved indefinitely pending further notice from the U.S. Department of Justice. All HIX related activities are currently awaiting a National Archive and Records Administration (NARA) approved schedule.

EACMS also abides by National Archives and Records Administration (NARA) General Records Schedule 3.2 (GRS 3.2) for Electronic Records of users for authorization and ID management such that they will be

destroyed/deleted 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 (Disposition Authority, N1-GRS-07-3, item 13a2); and

deleted/destroyed when agency determines they are no longer needed for administrative, legal, audit or other operational purposes (Disposition Authority: N1-GRS-07-3, Item 13b).

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

Physical: This includes multiple physical security measures within data centers. This includes 24/7 Security Staff and Physical Access Control System (PACS) using Secure-Card Key Access, Biometric Scanners, and Alarmed Door.

Technical: Encryption for all backup tapes and data connections, and data base encryption at the field level. Additionally, multiple intrusion detection and prevention methodologies are employed, and the system is tested regularly (multiple times a year) for application vulnerabilities, and daily for

system vulnerabilities.

Administration: Policies and Procedures have been created on securing PII in the EACMS system. An example of these are Security Awareness and Training (SAT) policies, policies on the storage of PII, access control policies are used for login access, policies for following the NARA record retention policy. Also, EACMS has policies on continuous monitoring of the system and audit log reviews.