US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/06/2026

OPDIV:

CMS

Name:

Medicare Part B Shared System Claims Processing Maintenance

PIA Unique Identifier:

P-1907179-364033

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.

Significant System Management Change

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

The MCS Dev/Test applications are located at the CMS IaaS-CACHE Kent, WA Datacenter and do not collect, maintain, use or share "live" PII / PHI.

The MCS Production and UAT application environments and related security boundary are managed by the Kent/Ashburn Fee-for-Service Medicare infrastructure Service Provider (MiSP) contractor who is Companion Data Services (CDS). CDS holds the MiSP contract for the Medicare Part A, Part B and DME applications. The MiSP provides support for the Kent Data Center (WDC* LPAR) FFS Workload A and the Ashburn Data Center (EDC* LPARs) FFS Workload B environments. Leidos, acting as another MiSP, provides services for operations, management, and continuous monitoring of security controls protecting the MCS Production environment (WDC*/EDC*) where live PHI/PII data are processed, stored, and transmitted by the users of the system (MACs).

Describe the purpose of the system.

Medicare Part B Shared System Claims Processing Maintenance, also known as the Multi-Carrier System (MCS) is the shared system used to process Medicare Part B claims for physician care, durable medical equipment, and other outpatient services nationwide. The Medicare Part B claims processing includes data collection and validation, claims control, pricing, adjudication, correspondence, on-line inquiry, file maintenance, reimbursement, and financial processing. MCS connects to the CMS system Common Working File (CWF) so that the MCS users will not be required to exit the system to retrieve information pertaining to eligibility, Medicare Secondary Payer (MSP), health maintenance organization, deductible status, and other key CWF data elements.

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

The information in MCS includes name, date of birth, social security number, mailing address, phone numbers, medical record numbers, medical notes, financial account information and/or numbers, certificates, device identifiers, email address, military status, employment status, education records, health insurer name/plan, health insurer group number, patient marital status, and claims forms for the purpose of processing and paying claims.

MCS manages the system's user credentials. Users are CMS employees and direct contractors. User credentials are user ID and password and are synchronized by the CMS Enterprise User Administrator system (EUA).

Since MCS is a batch processing application, there are no user accounts for the system. The MCS host facility in Kent, Washington maintains administrative accounts for users maintaining the host site infrastructure, but they do not access the MCS system.

Administrative accounts are validated via EUA. EUA is covered by a PIA managed by the Infrastructure and User Services Group (IUSG). User authentication data collected is username and user password.

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

MCS provides ongoing Medicare Part B claims for physician care, durable medical equipment, and other outpatient services, nationwide claim support, and system maintenance. The information collected, maintained or disseminated includes test data, change requests to the application code or system and patient claims processing.

The MCS Test and Development System requires User system login credentials for identifications and authentication to retrieve system records.

MCS regularly retrieves information by the beneficiary's name, Health Insurance Claim Number (HICN), and assigned unique physician identification numbers.

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

Medical Records Number
Medical Notes
Financial Accounts Info
Certificates
Education Records
Device Identifiers
Military Status
Employment Status
Health Insurer name/plan, Health insurer group number, Patient marital status, Claims forms, User credentials, Physician identification numbers, Medicare Beneficiary Identifier, User Credentials. Administrative accounts are validated via EUA. EUA is covered by a PIA managed by the Infrastructure and User Services Group (IUSG).

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

Employees
Public Citizens
Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Information is shared to verify patient data between Medicare Insurers, if necessary, as well as beneficiary entitlement and accuracy of payment.

Internal system user's PII is collected to verify the system user's identity and credentials.

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

The information is used in the development and testing of the application while it resides at the contractor data center

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

Sections 1816, and 1874 of Title XVIII of the Social Security Act (42 U.S.C.1395h, and 1395kk).

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.

Medicare Multi-Carrier Claims System, 09-70-0501.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Online
Government Sources
Within OpDiv
Non-Governmental Sources
Public

Identify the OMB information collection approval number and expiration date

OMB CONTROL NUMBER: 0938-1197
Expiration Date: 10/31/2027

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.

For the beneficiary, written notice is given when the beneficiary initially enrolls in the Medicare program and written or orally each time the beneficiary applies for service at a provider.

For the MCS system users, written notice is provided as part of the employment process.

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.

When a beneficiary's data is collected and sent to the MCS system, the beneficiary has already agreed to share their information, so there is not an ability for them to opt out of PII data collection.

The MCS system users cannot opt out of providing PII because it (user credentials) is necessary to access the system.

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

Due to the large number of beneficiaries and providers that would be impacted by a change, obtaining individual consent is not feasible. Therefore, in accordance with the Privacy Act, a new SORN would be published with a 60-day comment period to notify individuals of a change in use and/or disclosure of data by the MCS system.

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 are notified annually in the Medicare & You handbook of their right to file a complaint if they believe their privacy rights have been violated. A phone number is included in the handbook and there is more information on www.medicare.gov. The phone number is 1-800-Medicare.

For system users, they would contact the CMS IT help desk either by telephone or email and describe the issue. The IT help desk will investigate and determine how to resolve the concern.

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 is maintained through system security and control processes that are reviewed by external auditors. Availability is maintained through system redundancies and MCS is required to annually test disaster recovery capabilities. Relevancy and accuracy are maintained by the interactions with the systems - Fiscal Intermediary Shared System (FISS) and Viable Information Processing Systems (ViPS) Medicare Shared System (VMS).

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.

MCS uses role-based access limitations and least privilege controls to restrict PII availability. Role-based job codes must be applied for and approved by the designated approvers prior to access being granted.

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.

CMS administrators and direct contractors have role-based access which limits their access to PII data. Users must have an MCS job code in their EUA user profile before they are granted access to MCS.

MCS employs the CMS Enterprise User Administration and Resource Access Control Facility (RACF) to issue user IDs and grant permissions. Data center administrators have role-based access, which limits their access to PII data. EUA is covered by a PIA managed by the Infrastructure and User Services Group (IUSG).

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.

Security Awareness and Privacy training is required for CMS employees and direct contractors on an annual basis. Users acknowledge successful training after passing a test at the end of training and the system verifies completion. Included in the training is education about how to properly handle sensitive data.

Security personnel receive job-related training by attending conferences, forums, and other specific training on an annual basis. Security based role training is recorded within the security department.

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

MCS staff receive annual incident response training and acknowledge security rules of behavior. Security staff may receive additional training throughout the year from CMS and outside providers as training is scheduled/becomes available. MCS production staff maintain their own training programs and training records of their personnel.

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.

Per National Archives and Records Administration (NARA) Disposition Authority N1-440-09-14: PII records are retained temporarily. Cutoff at the end of the fiscal year (FY). Delete/destroy 6 years and 3 months after cutoff, or when no longer needed for Agency business, whichever is later.

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

The administrative controls include access to the systems is given based on need to know and job responsibilities; system maintainers use security software and methods to provide “least privilege access.” External audits also verify these controls.

Technical controls used include user identification, passwords, firewalls, virtual private networks and intrusion detection systems.

Physical controls used include guards, identification badges, key cards, cipher locks and closed-circuit televisions.