US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/23/2026

OPDIV:

CMS

Name:

Fiscal Intermediary Shared System (ATO)

PIA Unique Identifier:

P-6651713-848618

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.

Fiscal Intermediary Shared System (FISS) Development/Test applications are located at the CMS Infrastructure as a Service (IaaS) - Continuously Available CMS Hosting Environment (CACHE) Kent and do not collect, maintain, use or share "live" PII / PHI.

The FISS Production and User Acceptance Testing (UAT) application environments and related security boundary are managed by the Kent/Ashburn Fee-for-Service (FFS) 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 Durable Medical Equipment (DME) applications. The MiSP provides support for the Kent Data Center (West Data Center (WDC) Logical Partion (LPAR)) FFS Workload A and the Ashburn Data Center (East 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 FISS Production environment (WDC/EDC)

where live PHI/PII data are processed, stored, and transmitted by the users of the system - Medicare Administrative Contractors (MACs).

Describe the purpose of the system.

The Fiscal Intermediary Shared System (FISS) application is the shared system used to process Medicare Part A claims for physician care, durable medical equipment, and other outpatient services nationwide. It processes Medicare Part A claims, to include data collection and validation, claims control, pricing, adjudication, correspondence, on-line inquiry, file maintenance, reimbursement, and financial processing.

It interfaces directly with the Common Working File (CWF). The Common Working File (CWF) is a tool used by the Centers for Medicare & Medicaid Services (CMS) to maintain national Medicare records for individual beneficiaries enrolled in the program. The system is used to determine the eligibility of patients and to monitor the appropriate usage of Medicare benefits. This is also the repository for the beneficiary data received nightly from the Social Security Administration. CWF is covered by a separate Privacy Impact Assessment (PIA).

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

The information collected, maintained or disseminated includes name, date of birth, health insurance claim number, mailing address, phone numbers, medical record numbers medical notes, financial account information and/or numbers, certificates, device identifiers, email address, military status and/or records, employment status and/or records, employer or school name, education records, health insurer name/plan, health insurer group number, patient marriage and employment status; claims forms for the purpose of processing and paying claims.

User ID and Password for system users (CMS employees and direct contracting support) are managed by FISS. The FISS Users IDs and Passwords are synchronized by the CMS Enterprise User Administrator system (EUA) to CMS IDs.

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

The FISS subsystem, Medicare Part A Shared System Maintainer (SSM), manages the Claims Processing application system (known as FISS) to provide ongoing 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.

Test data is composed of collected data items to make test records that can simulate actual claims records. The test data used accurately reflects all possible claims conditions to ensure that changes to the application do not disrupt claims processing.

The real data is supplied by the Social Security Administration (SSA) and satellite batch processing

sites.

The system stores information about its system users for authentication, access control, auditing and reporting purposes.

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

FISS regularly retrieves information by the beneficiary's name, Health Insurance Claims Number (HICN), and assigns unique physician identification number.

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
Medical Records Number
Medical Notes
Financial Accounts Info
Certificates
Education Records
Device Identifiers
Military Status
Employment Status
Employer or school name, Health Insurer Name/Plan, health insurance claim number, Health Insurer Group Number, Patient Marriage, and Employment Status, 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
Vendor/Suppliers/Contractors
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.

System user credentials are used for authentication, access control, auditing and reporting purposes.

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

The information is used in the Development and Testing of the claims processing application to use test data to make test records that can simulate actual claims records. This is being done to ensure that changes to the application do not disrupt claims processing as it resides at the contractor data

center.

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

Sections 1816, 1862 (b) and 1874 of Title XVIII of the Social Security Act (the Act) (42 U.S.C. 1395 (h), 1395y (b), 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.

The FISS System of Records Notice (SORN) is 09-70-0503; Common Working File SORN is 09-70-

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within OpDiv

Other Federal Entities

Identify the OMB information collection approval number and expiration date

OMB approval is not applicable to direct collection of system user credentials.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

There are Computer Matching Agreements (CMAs) in place between CMS and SSA, IRS, RRB and participating States.

FISS shares/collects information from other CMS systems only within the CMS datacenter. MOUs are not required for CMS systems authorized under the same authorizing official.

The Computer Matching and Privacy Protection Act (CMPPA) Agreement (Agreement) establishes the terms, conditions, safeguards, and procedures under which the Social Security Administration (SSA) will disclose information to the Centers for Medicare & Medicaid Services (CMS) under the Patient Protection and Affordable Care Act (Public Law (Pub. L.) No. 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Pub. L. No. 111-152)

Computer matching agreements (CMA) establish the conditions for data sharing between CMS and the Railroad Retirement Board, Treasury department and others. A CMA is a written agreement between the source agency and the recipient agency (or non-federal agency) specifying the terms of the matching program. The computer matching provisions of the Privacy Act apply to a broad range of federal agency computer matching activities for the purpose of establishing or verifying eligibility or compliance as it relates to cash or in-kind assistance or payments under federal benefit programs.

These agreements are executed in compliance with the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, and the regulations and guidance promulgated thereunder. The legal authority for the disclosures under this agreement is the Privacy Act of 1974, as amended (5 U.S.C. § 552a(b)(3)), which authorizes a federal agency to disclose information from its system of records, without prior written consent, when such disclosure is pursuant to a routine use.

Describe the procedures for accounting for disclosures.

CMS has safeguards in place for authorized users and monitors such users to ensure against unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

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 CMS contractors and CMS employees, written notice is provided when they apply for a job.

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 FISS 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 CMS contractors and CMS employees cannot opt out of providing PII because the collection of the data is necessary for employment.

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 System of Record Notice (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 FISS system.

The term "system of records" (SORN) means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

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. When a beneficiary calls this number, they are contacting a CMS system known as the Next Generation Desktop (NGD), which is a system that is separate from the FISS. To resolve complaints, CMS Contractors log onto the NGD system to retrieve and respond accordingly to complaints. The final resolution is managed and recorded in the NGD system. NGD is covered by a separate privacy impact assessment (PIA).

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

FISS does not collect personally identifiable information (PII) from individuals; the data is supplied by the Social Security Administration (SSA) and satellite batch processing sites. Relevancy and accuracy are maintained by interactions with the other claim data systems.

Integrity is maintained through system security and control processes that are reviewed by external auditors. Availability is maintained through system redundancies and FISS is required to annually test disaster recovery capabilities.

Only Systems Administrators have access to make authorized changes and system security audit logs capture all changes made by privileged users. Logs are reviewed to ensure all security changes have been approved as part of the formal change management process.

System Administrators maintain/manage user system account information by periodic reviews, accounts are disabled and then removed during the termination process or when no longer needed. User accounts are maintained by the Operating system and only system administrators can access the information.

System security audit logs capture the user IDs of the systems administrator who makes changes to user accounts.

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.

FISS uses role-based access limitations and least privilege controls to restrict PII availability.

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.

Administrators and Direct Contractors have role-based access which limits their access to PII data.

Users must have a FISS job code in their EUA user profile before they are granted access to FISS.

FISS 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 provided to each user 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.

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

FISS 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. FISS 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.

Data within FISS is temporarily retained by the National Archive Records Administration (NARA) Disposition Authority: N1-440-09-16, Item 2: Cutoff at the end of the fiscal year in which cost reports are produced. Delete/destroy 8 years after cutoff, or when no longer needed for Agency business, whichever is later and per NARA Disposition Authority: N1-440-09-8: Cutoff at time of annual update. Delete/destroy each annual data file 10 years 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.

Access to the systems is given based on need to know and job responsibilities to process Medicare claims. Medicare Claims Processing Standard Systems maintainers use security software and methods to provide “least privilege access.” They will utilize software which is part of the security systems that provides access control and auditing functionality, the ability to grant or deny access to data based upon need to know. Sometimes, to fix programmatic problems, programmers are granted temporary access to fix and ensure that errors are fixed. Temporary access may be granted for a day or other short periods of time that can be controlled through security software. 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.