US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/06/2026

OPDIV:

CMS

Name:

Strategic Work Information Folder Transfer System

PIA Unique Identifier:

P-9970293-422480

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

Internal Flow or Collection

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

There is a new SWIFT application, Inquiry Management System (IMS), which supports beneficiary inquiry processing, including integration with the Digital Mail System for inquiries received via mail.

There is a new SWIFT application, Outgoing Mail, which facilitates the preparation and submission of outgoing letters. Supports validation, printing, folding, and envelope insertion with high-speed equipment.

Describe the purpose of the system.

The Strategic Work Information and Folder Transfer (SWIFT) system is an enterprise-grade case and workflow management platform used across multiple HHS Operating and Staff Divisions, including CMS. It centralizes many types of cases enabling agencies to track, process, and collaborate on complex workloads with efficiency, transparency, and accountability.

SWIFT provides multiple specialized applications on a shared platform:

Case and document management for correspondence, regulatory materials, Freedom of Information Act (FOIA) requests, beneficiary inquiries, litigation holds, and more.

Automated workflow and routing with due dates, multi-office collaboration, and status visibility.

Advanced search, dashboarding, and reporting to quickly access and analyze cases.

Digital mail processing for incoming and outgoing correspondence, eliminating paper-based delays.

Secure public portals for FOIA and Privacy Act requests.

SWIFT supports CMS users in Central and Regional Offices nationwide, as well as Medicare Administrative Contractors (MACs) and other partner organizations.

Core Applications

1. Correspondence Tracking System (CTS)

Tracks and manages executive correspondence, memos, and reports to Congress from receipt through clearance and final signature. Supports workflow and deadline management, collaboration, dashboards, and custom notifications.

2. Inquiry Management System (IMS)

Supports beneficiary inquiry processing, including integration with the Digital Mail System for inquiries received via mail.

3. FOIA Management System

Full lifecycle request tracking, de-duplication, fee management, processing time tracking, and annual reporting.

4. FOIA Public Portal

Guides the public through online submissions, status checks, and referral routing.

5. FOIA Contractor Portal (FCP)

Enables MACs to securely receive, process, and report FOIA requests.

6. Digital Mail System

Digitizes and securely delivers incoming paper mail to the correct CMS component mail stops.

7. Outgoing Mail System

Online portal for preparing and submitting outgoing letters. Supports validation, printing, folding, and envelope insertion with high-speed equipment.

8. Litigation Holds

Facilitates legal “do not destroy” notifications and approvals, leveraging SWIFT’s paperless approval process.

9. Regulations Management System (RMS)

Manages regulation planning, clearance, and comment tracking. Supports collaborative editing, multiple clearance rounds, milestone tracking, and reporting.

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

The SWIFT Correspondence application contains data and documents related to incoming letters from external parties or correspondents, such as individuals in Congress or from citizens. The system collects and maintains Personally Identifiable Information (PII) such as names, addresses, email addresses, phone numbers, Organizations, HICN (Health Insurance Claim Number), and MBI (Medicare Beneficiary Identifier) in requests when voluntarily provided by correspondents. HICN and MBI are only available on the beneficiary Inquiry document type where the business need exists for those data elements. Due to the sensitive nature of the attribute, the HICN cannot be exported to reports to protect it from inadvertent disclosure. Documents and/or letters voluntarily provided by the requestor may contain other PII including Social Security Numbers (SSN). However, PII in documents is not captured or displayed on any web pages available to the user (i.e. PII in documents is not captured in structured data elements).

The FOIA application contains data and documents related to incoming FOIA requests. The system also contains the response records to incoming requests and includes information requested under the Freedom of Information Act. The system collects and maintains PII such as names, addresses, email addresses, and phone numbers voluntarily provided by requestors. Documents and/or letters voluntarily provided by the requestor may contain other PII including Social Security Numbers (SSN). However, PII in documents is not captured or displayed on any web pages available to the user (i.e. PII in documents is not captured in structured data elements). All FOIA records in SWIFT are removed in accordance with the Agency’s records management schedule then forwarded to the National Archives and Records Administration (NARA).

The FOIA Public Portal collects data and documents supplied by the public needed to fulfill a request for the Medicare beneficiary records for the requestor or on behalf of the requestor. The requests are routed to the SWIFT FOIA application where they are managed. No data or documents are stored on the FOIA Public Portal server. The data collected includes PII such as first name, last name, MBI,

address, From Organization, email address, phone number, and fax number. Documents and/or letters voluntarily provided by the requestor may contain other PII including Social Security Numbers (SSN). However, PII in documents is not captured or displayed on any web pages available to the user (i.e. PII in documents is not captured in structured data elements).

The information in Litigation Holds is collected to assist Executives in approving Litigation Holds Memorandums. Litigation Holds does not collect or maintain any PII.

The Regulations Management System (RMS) application contains data and documents pertaining to regulations that are being authored and cleared by CMS. RMS does not collect or maintain any PII.

The Digital Mail and Outgoing Mail application contains digitized mail addressed to CMS in PDF format. The system collects and maintains PII such as the sender's name and address. The scanned images of the mail as well as any documents and/or letters voluntarily provided by the sender may contain other PII including Social Security Numbers (SSN). However, PII in scanned mail and documents is not captured or displayed on any web pages available to the user (i.e. PII in documents is not captured in structured data elements). All digitized mail items in SWIFT are considered temporary records because SWIFT is not the system of record for Digital Mail. The information is kept in SWIFT for three (3) years, then destroyed after review and signature by the business owner.

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

The information in the SWIFT Correspondence application is collected to route and process correspondence/requests and to respond to the submitter. The HICN and MBI are needed to enable CMS employees to search on these numbers to identify the correspondent. Records can be retrieved by the correspondent's name, address, email address, phone number, organization, HICN, and MBI.

The information in the FOIA application is collected to identify the person making the FOIA request so that the requestor's response records can be provided. Records can be retrieved by the requestor's name, address, email address, organization, or phone number.

The information collected by the FOIA Public Portal is used to transmit into SWIFT FOIA a request for the Medicare beneficiary records for the requestor or on behalf of the requestor. No information is stored or maintained within the portal. All information is transmitted into the existing SWIFT FOIA system as a new case with the same data elements as any other case created by other methods.

The information in Litigation Holds is collected to assist Executives in approving Litigation Holds Memorandums. Litigation Holds does not collect or maintain any PII.

The information in the Regulations Management System (RMS) application is collected to author and clear regulations for CMS. RMS does not collect or maintain any PII.

The information in the Digital Mail application is collected to record who sent the mail and to distribute the mail to the correct recipient(s). Mail is only delivered through SWIFT; no mail is responded to through SWIFT. Records can be retrieved by the sender's name, address, or organization.

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
Name
E-Mail Address
Mailing Address
Phone Numbers
MBI - Medicare Beneficiary Identifier; HICN – Health Insurance Claim Number, fax number, SSN, Organization. Unsolicited PII may also be collected, maintained, and stored in the system.

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

Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
beneficiaries

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

The primary purpose of collecting PII in SWIFT is to identify individuals corresponding to HHS / CMS and to identify Freedom of Information Act (FOIA) details used to properly respond back to those individuals. PII is collected when it is voluntarily provided by individuals and it is used to accurately respond.

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

Secondary uses of the PII are to identify requests from the same requester or that seek records about the same individual(s) to reduce duplicative records.

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

42 CFR 401.101–401.148, 1106(a) of the Social Security Act, 42 U.S.C. 1306(a) and E.O. 9397.

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.

09-90-1901 HHS Correspondence, Comment, Customer Service, and Contact List Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Hardcopy
Email
Online
Government Sources
Other HHS OpDiv
State/Local/Tribal
Non-Governmental Sources
Public
Media/Internet
Private Sector

Identify the OMB information collection approval number and expiration date

Approved under OMB control number 0938-0568. Currently in a renewal process.

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.

The Correspondence module shares information with the Secretary's Policy System (SPS) at the Immediate Office of the Secretary. An Interconnection Security Agreement (ISA) has been documented between The Office of the Secretary and CMS for secure information flow through the SWIFT and SPS system.

Describe the procedures for accounting for disclosures.

CMS never discloses a record for a reason other than FOIA.

This is an internal system to CMS, only CMS employees and authenticated contractors have access to SWIFT. Although the FOIA Public Portal is a public-facing website, no FOIA records are provided to the requestor through the website.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Individuals are notified by SORN 09-90-1901 HHS Correspondence, Comment, Customer Service, and Contact List Records
SORN history: 86 FR 12699 (3/4/21)

The policy governing the FOIA Public Portal is the FOIA Paperwork Reduction Act (PRA) Package (OMB control number 0938-1419). A PRA Disclosure statement is available on the FOIA Public Portal web site notifying users that their personal information will be collected.

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.

The constituent may opt-out of the collection of their PII by not signing the Privacy Act release form and not providing the information. However, the constituent is informed by the assigned Region or Component that to fully address their concerns this information may be needed.

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

After Correspondence and FOIA requests are fulfilled there is no longer a need for the requester's PII. All FOIA records in the SWIFT tracking system are removed in accordance with the Agency's records management schedule then forwarded to the National Archives and Records Administration (NARA). Requesters are notified about major system changes that impact the use of PII through a revised System of Record notice in the Federal Register.

CMS SWIFT users receive email notifications about major system changes and maintenance releases.

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 a concern or complaint may contact the Freedom of Information Group and reasonably identify the record and specify the information to be contested, state the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7.) Contact CMS FOIA Office Service Center, (410) 786-5353, fax (443) 380-7260.

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

No process exists since records are only used to answer the constituent's inquiry and are no longer needed nor used upon completion of the case. This process can take anywhere from 10 to 30 business days for the case to be closed.

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 Business Owner and SWIFT Contractor adhere to the principles of least privilege and the separation of duties when deciding which users may access PII. The Business Owner limits the users to employees who require access to PII to accomplish their job responsibilities. The SWIFT Contractor assigns contractor personnel to the appropriate role for their job responsibilities. SWIFT System Administrators handle daily operations and maintenance including user account creation and trouble shooting. Tier III personnel have create, read, update, and delete (CRUD) access to the SWIFT data.

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 Business Owner and SWIFT Contractor adhere to the principles of least privilege and the separation of duties when deciding which users may access PII.

Additionally, within the SWIFT Correspondence application, there are two types of roles - power user and gatekeeper. The Business Owner determines which employees are assigned to each role based on their job responsibilities. A power user can create and edit folders, refer folders to other components or gatekeeper boxes, add documents to folders, perform searches and close out folders. Gatekeepers do not have the ability to create or edit the folder data. They can respond to assignments given to them by the power users. When they respond they can add documents to the response which is added to the folder. Gatekeepers can perform a read only search of all the folders.

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.

Annual mandatory privacy and security awareness training is required for all CMS users and contractors that access the CMS network.

Annual mandatory Role-Based Training (RBT) is required for all Contractors with elevated privileges.

Rules of behavior for the SWIFT system are reinforced every time the system is accessed.

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

New SWIFT users are trained at their desks or over ZOOM on basic SWIFT operation. Group training is also provided by the Contractor on an as-needed basis. Additional group and advanced training is provided as new updates are implemented.

Annual mandatory Role-Based Training (RBT) is required for all Contractors with elevated privileges.

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 is stored and destroyed following the CMS Records schedule which follows NARA General Record Schedules (GRS). GENERAL RECORDS SCHEDULE

GRS 5.1: Common Office Records 010 Administrative records maintained in any agency office-- per Disposition Authority: DAA-GRS-2016-0016-0001. Temporary. Destroy when business use ceases.

GRS 5.1 Common Office Records 020 Non-recordkeeping copies of electronic records- per Disposition DAA-GRS-2016-0016-0002. Temporary. Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use.

GRS 5.1 Common Office Records 030 Records of non-mission related internal agency committees- per Disposition DAA-GRS-2016-0016-0003. Temporary. Destroy when business use ceases.

GRS 5.2 Transitory and Intermediary Records 010 Transitory Records- per Disposition DAA-GRS-2017-0003-0001. Temporary. Destroy when no longer needed for business use, or according to agency predetermined time period or business rule.

GRS 5.2 Transitory and Intermediary Records 020 Intermediary Records- per Disposition DAA-GRS-2017-0003-0002. Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Notes and Exclusions apply to retention schedules listed above. For more information, please refer to the appropriate retention schedule.

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

Administrative controls:

The Business Owner and SWIFT Contractor adhere to the principles of least privilege and the separation of duties when deciding which users may access PII. The request and approval of access is controlled through the CMS End User Agreement (EUA) system and role-based functions for individual users.

Technical controls:

The system sits behind the HHS firewall (meaning only accessible within the HHS network), multi-factor authentication is used in conjunction with an Active Directory, all traffic is encrypted, audit logs are in place, and anomalous activity is monitored (e.g. system activity outside specific hours). Accounts are maintained in an encrypted data storage facility using Active Directory tools. Accounts are only accessible by administrative personnel who have established user ID and password.

Physical controls:

The physical controls include door locks, personnel badges and security guards at the data center where the system resides.

Identify the publicly-available URL:

https://foia-request.cms.gov/

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?

No

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?

No

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

null