PTA / PIA: HRSA - SWIFT - QTR3 - 2025 - HRSA1446247

Created Date: 10/15/2025 8:23 AM Last Updated: 3/16/2026 4:22 PM

General Information

PTA / PIA Name:	HRSA - SWIFT - QTR3 - 2025 - HRSA1446247	**PTA / PIA ID:**	3913422
Component Name:	HRSA - Strategic Work Information and Folder Transfer System	**ATO Boundary Name:**	Strategic Work Information and Folder Transfer System
Overall Status:	Complete	**# of Days - Open:**	251
Submitter:		**Submit Date:**	12/15/2025
Next Assessment Date:	03/15/2029	**Expiration Date:**	3/15/2029
Office:		**OpDiv:**	HRSA
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	9/7/2023
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Michael Makinde Rebecca Andam
PTA 01A:	POC Title and Organization	ISSO, HRSA
PTA 01B:	POC Email Address	MMakinde@hrsa.gov
PTA 01C:	POC Phone Number	301-370-9562
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	No changes since last PIA

PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The Strategic Work Information and Folder Transfer (SWIFT) Correspondence System is an electronic document management system being used for the following types of documents and actions: Regulations, Reports to Congress, Correspondence, Memoranda to the Secretary, Deputy Secretary, Chief of Staff and Executive Secretary, Briefings for the Secretary, Deputy Secretary, and Chief of Staff and Invitations to the HRSA Administrator. The SWIFT Freedom of Information Act (FOIA) System is an electronic document management and workflow system that will process various FOIA requests received by the FOIA office. It will permit the vast majority of documents to be collected, reviewed and/or mailed as PDF's. In 2021, the FOIA system was enhanced to integrate with the DOJ FOIA web site (FOIA.gov) to enable FOIA requests for HRSA to be entered on the FOIA.gov web site. In 2022, the FOIA system was enhanced to integrate with the FOIA Public Portal (a new standalone public facing web site) specifically created for requesting HRSA FOIA requests.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The system collects and maintains the following types of documents and actions: Regulations, Reports to Congress, Correspondence, and Memorandum to the Secretary, briefing, and FOIA requests. Secondary Personal Identifiable Information such as , Name, Driver's License Number, Electronic Mail (E-Mail) Address, Mail address, Financial Account Info, Legal Documents, and Employment Status may be collected as part of FOIA request and correspondences. SWIFT is used by all Bureaus and Offices throughout the Agency as a means of increasing the efficiency of the controlled correspondence process. All data and documents stored in SWIFT are retained according to the defined records management schedule. Users (HRSA employees and direct contractors) access SWIFT with their HRSA credentials.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	User credentials access is managed by HACAP/AMS with HRSA AD

PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The system collects and maintains the following types of documents and actions: Regulations, Reports to Congress, Correspondence, and Memorandum to the Secretary, briefing, and FOIA requests. Secondary PII such as Name, Driver's License Number, E-Mail Address, Education Records, Date of Birth, Mail address, Financial Account Info, Legal Documents, Military Status and Employment Status may be collected as part of FOIA request and correspondences. SWIFT is used by all Bureaus and Offices throughout the Agency as a means of increasing the efficiency of the controlled correspondence process. All data and documents stored in SWIFT are retained according to the defined records management schedule.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	Production: https://swift.hrsa.gov QA: https://swifttest.hrsa.gov foia.hrsa.gov
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes
PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	SWIFT web site (swift.hrsa.gov; internal to HRSA): Purpose: The purpose of the SWIFT web site is described in PTA-8. Who has access and how: HRSA SWIFT Users access SWIFT using an internal url. The user's HRSA credentials are authenticated by the HRSA HACAP system. The authenticated user's HRSA username is passed to SWIFT to compare to the SWIFT database of valid users. System Administrators access the SWIFT servers using HRSA Personal Identification Verification (PIV) and Alternate (ALT) cards and elevated accounts. No HRSA Government Furnished Equipment (GFE) is required. Contractors (Support Personnel) access SWIFT using HRSA PIV cards and HRSA GFE. FOIA Public Portal web site (foia.hrsa.gov; public-facing): Purpose: The purpose of the FOIA Public Portal web site is to allow the general public to submit FOIA requests to HRSA. Who has access and how: Public users access the FOIA Public Portal using the internet. Users do not have to create a account so no authentication needs to occur. System Administrators access the FOIA Public Portal server using HRSA PIV and ALT cards and elevated accounts. No HRSA GFE is required. Contractors (Support Personnel) access the FOIA Public Portal using the internet. No HRSA GFE is required.
PTA 10:	Does the website have a posted privacy notice?	Yes

PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Driver's License Number Financial Account Information (e.g., account numbers, credit card numbers) Biographical Information Name User Credentials Employment Status/History Legal Documents Contact Information Email Address (Business) Mailing Address (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	5,000 – 9,999

PIA 25:	For what primary purpose is the PII used?	SWIFT is used to track responses and correspondence, which can include providing information, policy interpretations, responses to journalistic inquiries, and many other kinds of correspondence. PII may be shared with appropriate points of contact in order to respond to the correspondence. Correspondence may include inquiries, requests for resolution of concerns, or any other matter. The information is shared with offices within the Department of Health and Human Services (HHS) who may be able to assist in appropriately responding to correspondence sent to the Secretary or FOIA requests received by HRSA. SWIFT is also used to track and fulfill requests received under the Freedom of Information Act (FOIA). The primary purposes for which PII is used are to document and analyze requests received from individual requesters or that seek records about individuals, locate responsive records about individuals, verify the identity of individual requesters, contact requesters, locate cases in the system (e.g., to manage cases or provide status information to requesters), process responsive records containing PII, maintain clean, marked and redacted versions of the processed records, and document responses to requests, including fee issues.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	NA
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 U.S.C. § 301, 5 U.S.C. 552, and 5 U.S.C. 552a, and Departmental Regulations.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	Name Email Address Date of Birth Drivers License
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	Secretariat's CORR Control System: 09-90-0037 Tracking Records and Case Files for FOIA and Privacy Act Requests and Appeals: 09-90-0058
PIA 30:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Other HHS OPDIV
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No

PIA 31B:	Explain why an OMB information collection approval number is not required.	N/A. Information in the system does not require answers to any questions and is not collected in a specific format that will require the Office of Management and Budget information collection approval.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies Private Sector Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	Within HHS: To route and process correspondence and requests, records and report data containing PII, verify identity of FOIA requesters, and locate records pertaining to particular individuals. Other Federal Agency/Agencies: To effect FOIA consultations and referrals involving individual requesters and/or requested records containing PII. Private Sector: To comply with the submitter notice process with respect to financial or commercial records containing PII - this process shares with the submitter the records that the submitter originally provided to HHS, but may also share the identity of the FOIA requester.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	NA
PIA 32D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	The SWIFT system maintains an accounting of disclosures in that the dates, nature, purpose, names and addresses of each correspondence is captured by the system. Additionally, responses to FOIA requests are exempt from this requirement per 5 USC 552a (c)(1).)
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	SWIFT does not request PII from individuals and individuals can choose which contact information to provide. However, individuals are given the opportunity to opt-in to the collection of their information when they send PII themselves in the correspondence and requests provided through the system. As a result no need to provide an opt-out methods. Information is used for the purposes for which individuals request that it be used, which is to address concerns or request responses to inquiries and requests. If a person opts out of providing his/her name and/or organization, the name does not appear on these documents, and is labeled as "anonymous" for action. An individual whose PII is in records responsive to a FOIA request has no option to object to the inclusion of the records in the system.

PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	Major changes would need to be reflected in the System of Records Notice (SORN) and Privacy Impact Assessment (PIA), which would be available to the public.
PIA 36:	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 no process exists, explain why not.	Although this system is exempt from the Privacy Act "accounting of disclosures" requirement, an individual can make a FOIA request for the FOIA request log to identify any individuals and entities requesting records about him/her, a description of the records requested, and the dates of the requests. An individual's concern that his/her PII was inappropriately released to a FOIA requester would be reported within HHS as a privacy incident and would be analyzed to determine if an improper disclosure occurred; the concern would be responded to in writing; and remedial measures would be taken if an improper disclosure occurred.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	Information is used transactionally and there would be no value to periodic reviews and updates
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: HHS correspondence and FOIA staff, including liaisons in the Bureaus and Offices will have access to PII pertaining to files they handle. Administrators: User account maintenance and correspondence assignments and processing. Contractors: These contractors are direct contractors that operate on behalf of the agency and use the agency's credentials when doing so to perform system administration.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The SWIFT Administrators and developers are contractor employees who do not enter information into SWIFT. Only Government employees (users) review the correspondence received to enter PII into the system. System administrators and developers who are contractors will be able to see PII (name, organization and phone numbers) of users for account creation and troubleshooting problems only.

PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	System users are granted only the access necessary to perform their jobs. This level of access is granted based on each user's position description as identified on the employee's Official Form-8. In addition, the system is designed based on set permissions; therefore employee access and use are based on their need to know. A user will only have access to their SWIFT folders and documents that have been sent to them as information only by the authoring agency.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	Annual HHS Mandatory Cybersecurity Information Systems Security Awareness and Privacy Awareness training are required and documented as completed yearly by all HRSA and Contractor users of SWIFT. In addition prior to accessing the system each employee must accept the rules of behavior prior to accessing their computer system that gives them access to SWIFT. Administrators of SWIFT are also required and documented as have taken the Role-Based Training
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Users of the FOIA module receive specialized training on a regular basis at FOIA/PA conferences and workshops hosted by HHS, Dept of Justice, and outside vendors providing advanced instructions and guidance regarding safeguarding personal privacy information and avoiding improper disclosures of PII in particular contexts and with respect to specific types of records.

PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	Records are maintained indefinitely using the records management schedule. Hardcopies of correspondence are sent to a Retention Center. The authority is DAA-0468-2011-0006-0003 and the Master Files are permanent. Cut off of at the end of the fiscal year in which correspondence was created or received. Transfer to the National Archives in 4 year blocks immediately after cut off. National Archives and Records Administration (NARA) is determining the appropriate Records Control Schedule (RCS) Job Number for all of the PII maintained in the system and the PII should be maintained until a determination is provided. The applicable records schedule for the FOIA module is GRS 4.2, Information Access and Protection Records (formerly GRS 14); it prescribes retention periods ranging from approximately 2 years to 6 years after the date a case is closed. The system will be updated when a case is closed, will calculate when case records are eligible for destruction, and will generate a report of eligible cases each year, for use in deleting eligible electronic records and shredding eligible paper files. Official Correspondence files are permanent and the retention authority is HRSA DAA-0512-2014-004-0061. The cut-off date for these records is at the end of the calendar year in which the file is created and files are transferred to the National Achieves in 5-year blocks, 15 years after the cut-off. General Correspondence files are temporary and the retention authority is HRSA DAA-0512-2014-004-0062. The cut-off for these records at the end of the calendar year in which the file is created and files are destroyed 7 years after the cut-off. FOIA request files are temporary and the retention authority is GRS 4.2, Information Access and Protection Records (formerly GRS-14). It prescribes retention ranges from approximately 2 years to 6 years after the date a file is closed.

PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative: a. SWIFT collects PII information directly from an individual about whom the Information pertains, from government sources, and from third-parties acting on behalf of individuals. In the case of government sources, PII information is verified from the source data system. b. SWIFT directly collects PII information from letters sent to CMS through the mail/email, from the DOJ FOIA Portal, and from the FOIA Public Portal. c. Initial evaluation of PII holdings are done at the bureaus and offices prior to submission to the SWIFT application. Bureaus and offices applications establishes and follows a schedule for regularly reviewing those holdings at least annually to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish its purpose. PII that is found to be inaccurate or outdated is updated. d. SWIFT does issue guidelines for maximizing the quality, utility, objectivity and integrity of disseminated information. PII data is collected in the SWIFT system on the Correspondence and FOIA Data Entry panels. When a SWIFT record is created, the record-creation date is logged on the Correspondence and FOIA Data Entry panels. When any data is changed on a SWIFT Correspondence or FOIA record, the record-modification date is logged and displayed on the appropriate Data Entry panel. Today cases are not marked to indicate if they contain PII. All cases in SWIFT are treated as potentially containing PII either in data or documents. SWIFT identifies when each record/file that is maintained in the SWIFT Correspondence module is due for destruction, based on the retention schedule. SWIFT maintains each record/file in the SWIFT FOIA module for 6 years, based on the retention schedule. Technical: SWIFT implements MFA through AMS and uses a role-based system to allow access to the data, which includes PII. Physical: SWIFT servers are stored in a local HRSA data center with limited access. This a responsibility of the General Support System (GSS)

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	2/26/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	73

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	3/11/2026
SOP Review Comments:		**# of Days - SOP Review:**	13

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	3/12/2026
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 3/12/2026 All comment(s) were addressed. This PIA is ready for SAOP review and approval. Reviewer: Nestor Villafuerte 12/12/2025 Please see comments and update accordingly: PTA-5: Per PIA-22: please include "Medical Records" as one of the PII elements collected, store, and maintained in this system. PTA-8A: Per PTA8B, please include foia.hrsa.gov in your response. PIA-22: Per PTA-5, please list "SSN, Education Records, and Military status.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	3/16/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	4

SAOP Signature

Date	User	Type	Name	Original Value	New Value
3/16/2026 3:40 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 05	VILLAFUERTE, NESTOR	12/15/2025	Removed SSN, Education Records, and Military status.	
PTA 05	VILLAFUERTE, NESTOR	12/15/2025	Removed SSN, Education Records, and Military status.	
PTA 05	BLAND, CRYSTAL	12/15/2025	Removed SSN, Education Records, and Military status.	
PTA 05	BLAND, CRYSTAL	12/15/2025	Removed SSN, Education Records, and Military status.	