


General Information		
PTA / PIA Name:	HRSA - SF - PRF - QTR2 - 2025 - HRSA1445980	PTA / PIA ID: 3613641
Component Name:	HRSA - Salesforce Provider Relief Funds (PRF) Performance Reporting and Case Management System	ATO Boundary Name: CARES Provider Relief Fund Payment Portal
Overall Status:	Complete 	# of Days - Open: 143
Submitter:		Submit Date: 8/13/2025
Next Assessment Date:	11/19/2028	Expiration Date: 11/19/2028
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.	9/29/2024
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	Ernest Boakye
PTA 01A:	POC Title and Organization	Information System Security Officer (ISSO)
PTA 01B:	POC Email Address	eboakye@hrsa.gov
PTA 01C:	POC Phone Number	301-443-0413
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.	There is no change to the system since the last PIA
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency

<p>PTA 04:</p>	<p>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.</p>	<p>The purpose of the system is to inform Provider Relief Fund (PRF) recipients who received one or more payments exceeding \$10,000 in the aggregate of the data elements that they will be required to report as part of the post-payment reporting process. Please refer: https://www.hhs.gov/sites/default/files/post-payment-notice-of-reporting-requirements.pdf</p> <p>In addition, the purpose is also to allow rapid responses to provider inquiries with respect to the disputes of the payments and questions related to post performance submissions</p>
<p>PTA 05:</p>	<p>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.</p>	<p>The system will collect and maintain the following PII elements:</p> <ul style="list-style-type: none"> Provider Identity Information Taxation Identification number (TIN) National Provider Identifier (NPI) Provider Type Business Name, Doing Business As (DBA) Provider Address, Head Quarters (HQ) <ul style="list-style-type: none"> Street 1 Street 2 City State Zip Filing Contact Identify Filing Contact Name Filing Contact Title Filing Contact Phone Number Filing Contact Email Display Acquisition/Divestiture information pulled from profile Display Subsidiary TINs that provider will be reporting on from profile. Ask provider if Parent will be reporting on the General Distribution on their behalf. PRF Amount Received Display Payments to Provider Additional Provider Payment Information Financial Information: Un-reimbursed Expenses Financial Information: Lost Revenues Attributable to <ul style="list-style-type: none"> Coronavirus Patient Metrics Facility Metrics Survey Questions User Access Information Internal HRSA staff will be validated through AMS Providers will use email and password with multi-factor authentication through Salesforce mobile app Authenticator for verification.
<p>PTA 05A:</p>	<p>Are user credentials used to access the system?</p>	<p>Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.</p>
<p>PTA 05C:</p>	<p>Please identify the system that maintains the user credentials or controls access to this system.</p>	<p>HHS Access management System</p>

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 will collect the provider's identity information which will be used to create a profile and authenticate the provider for Case Management. It also has the provider's subsidiary profile and TIN. This information will be stored in Salesforce to keep track of the survey/reporting information on grant funds received by the organization. This information is collected for reporting purposes to ensure that disbursement of grant funds is tracked and analyzed for the use of COVID-19 care. This information is also viable to evaluating the use of emergency government funding for future pandemics. The system will collect all inquiry information to address any payment disputes or technical challenges the providers may have during their reporting. All information will be captured and stored in Salesforce within the boundary of the Government Cloud. This information will be stored in accordance with HRSA guidelines for records management.
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).	https://prfreporting.hrsa.gov/s/ https://commercialaudit.hrsa.gov/s/
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.	HRSA developed the PRF Reporting Portal to enable PRF and American Rescue Plan (ARP) Rural1 (referred to as "reporting entities" throughout this document) to comply with mandatory reporting requirements. Reporting entities must complete a two-step process in the PRF Reporting Portal (also referred to as "the portal" throughout this document) to submit their reports to HRSA. Providers and auditors access the application by accessing a public URL through the web browser and authenticate using username/password with MFA to log into the reporting portal
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?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies- Does Not Collect PII
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?	Yes
PTA 20A:	What TPWAs are used?	Google Recaptcha
PTA 20B:	Do the TPWAs have an approved TPWA PIA?	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.	<p>Identifying Numbers</p> <ul style="list-style-type: none"> Taxpayer ID Number (TIN) Financial Account Information (e.g., account numbers, credit card numbers) <p>Biographical Information</p> <ul style="list-style-type: none"> Name Employment Status/History <p>Contact Information</p> <ul style="list-style-type: none"> Email Address (Personal) Phone Numbers (Personal) <p>Other</p> <ul style="list-style-type: none"> Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	<p>NPI</p> <p>Provider Type</p> <p>Provider Address (HQ)</p>
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	<p>Employees/HHS Direct Contractors</p> <p>Members of the public</p>
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	To track organizations who have received federal coronavirus disease (COVID) funding for providing support in an effort to attend to COVID-19 patients.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	There is not any intention for using personally identifiable information (PII) for a secondary purpose.
PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	Tax identification number (TIN) is required to access the system and for the disbursement of the federal funds users are requesting.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	SSN is not used.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 U.S. Code (USC) 301, 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, E-Mail, Phone Number, Taxpayer ID, Mailing Address, Financial account info, employment status

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.	Provider Support Records, 09-15-0093 - https://www.federalregister.gov/documents/2021/11/26/2021-25760/privacy-act-of-1974-system-of-records
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Non-Government Sources Other
PIA 30A:	Identify the "other" sources of PII in the system not mentioned in the above list.	Providers
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.	Information collected into and/or maintained in the system is not subject to one or more Office of Management and Budget (OMB) Control Numbers.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
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.	For individual users of HRSA Provider Relief Fund (PRF) there is no opt-out to the collection and use of their PII as their TIN is required to access the system and for the disbursement of the federal funds they are requesting. A user who wishes to "opt-out" will not be granted a system account.
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.	When a HRSA CARES Act Provider subscribes to the Salesforce Provider Relief Funds Reporting System, the Provider is consenting to the collection and use of their information. Noted in HRSA PRF Privacy Policy.
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.	There is no process, as individuals are notified at the time they submit the information stored in HRSA PRF System that it will be used for legitimate purposes and it will not be disclosed unless authorized by law.
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.	Daily review is used to maintain accuracy of data.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers 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.	<p>Users: Users have access to only their own PII and those of their subsidiaries.</p> <p>Administrators: Admins are granted access for maintenance of the system.</p> <p>Developers: Only select developers with HRSA government furnished equipment (GFE) and access will have to use PII for prepare for user acceptance testing (UAT).</p> <p>Contractors: Direct Contractors with HRSA with personal identity verification (PIV)/Government furnished equipment(GFE) for development and operations of the system</p>
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	<p>SF-PRF control of information flow is done through the permissions built into the application. The security module prevents users from accessing data belonging to Programs that they are not assigned to, through the use of RBAC. Configuration of SF-PRF application permission sets include object level, field level and record-level security. These can prevent users from accessing, seeing, creating, editing, or deleting records and data.</p> <p>In accordance with the user's access control and role, each user will be uniquely identified and authenticated prior to accessing the systems. A successful authentication requires a user possess a valid PIV card within the HRSA infrastructure and a valid AMS account. SF-PRF is configured to leverage HHS AMS authentication services (interconnected from HHS) to identify and authenticate HRSA user (for PIV Access) and ensure their information is also resident within the AMS. These users may access PII assigned to them based on their roles. Non-Organization users (providers) are required to create an account that uniquely identifies them from the rest of the providers. Providers leverage their personal/organization email as their unique identification, which is used as their username when they login to SF-PRF. They are required to create a complex password, google reCAPTCHA, and set a two-factor authentication with a token. These non-organizational users can only access submitted PII under their provider's TIN.</p>

<p>PIA 41:</p>	<p>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.</p>	<p>All system users with access to the production environment will have read access to PII. Non-privilege users or end users will have access to only their submitted PII as dictated by their account and role. Privilege users such as system administrators have access to all PII within the system.</p> <p>SF-PRF enforces restrictions on system functionality (and data access) via Role Based Access Control (RBAC). The SF-PRF system admin/owners grant access permission on a need to know basis.</p> <p>SF-PRF control of information flow is done through the permissions built into the application. The security module prevents users from accessing data belonging to Programs that they are not assigned to, through the use of RBAC. Configuration of SF-PRF application permission sets include object level, field level and record-level security. These can prevent users from accessing, seeing, creating, editing, or deleting records and data. Permissions are set for a specific Profile.</p> <p>**Note - There may be a requirement to modify PII after reporting submission and during the Review process but this is not yet defined and may also be limited only to a notes field and not updating the actual PII data within the field.</p>
<p>PIA 42:</p>	<p>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.</p>	<p>All HRSA employees and direct contractors that use the HRSA PRF are required to take government-furnished annual security awareness training. All system users will receive system training and HRSA PRF user guides to support the various functions of the system.</p> <p>All HRSA employees and direct contractors that use the HRSA PRF System are required to take government-furnished annual security awareness trainings. Upon accessing the initial HRSA PRF System trainings all users will be required to acknowledge that they have completed all of the requisite HHS privacy trainings, including: the Annual HHS Information Systems Security Awareness Training; the Annual HHS Privacy Training; and have read the Rules of Behavior for Use of HHS Information Resources and signed the accompanying acknowledgment. Once the HRSA PRF System user acknowledges that they have completed the requisite privacy trainings, they will then be able to access the HRSA PRF System training materials which will in turn give them access to the HRSA PRF System. Without completing the privacy training acknowledgment, HRSA PRF System users will not be able to access the system.</p>
<p>PIA 43:</p>	<p>Describe the training system users receive above and beyond general security and privacy awareness training.</p>	<p>There is no additional formal training provided by HRSA.</p>

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).

PRF maintains all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and HHS/HRSA policies and shall not dispose of any records unless authorized by HHS/HRSA. In the event that PRF accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with HHS/HRSA policies. PII within HRSA PRF is stored as long there is a business purpose within the system for audit, legal, and customer use.

The records are not currently scheduled, so are retained indefinitely pending scheduling with the NARA. HRSA anticipates proposing a retention period of at least 6 years to NARA for the records, for consistency with General Records Schedule 1.1, Financial Management and Reporting Records, which provides for such records to be retained for 6 years after final payment or cancellation, or longer if required for business use.

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 controls. Management oversight of activities, security awareness and training for federal staff and direct contractors that use of the system, disaster recovery exercises, separation of duties for personnel administering the system, and isolating development test instances of the system.

These safeguards include protecting the facilities where records are stored or accessed with security guards, badges and cameras; controlling access to physical locations where records are maintained and used by means of combination locks and identification badges issued only to authorized users; limiting access to electronic databases to authorized users based on roles and either two-factor authentication or password protection; using a secured operating system protected by encryption, firewalls, and intrusion detection systems; and training personnel in Privacy Act and information security requirements.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	Privacy Analyst Review Date:	9/23/2025
Privacy Analyst Review Comments:		# of Days - PA Review:	41

SOP Review

SOP Review Decision:	Approved	SOP Review Date:	10/15/2025
SOP Review Comments:		# of Days - SOP Review:	22

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	Agency Privacy Analyst Review Date:	11/20/2025
Agency Privacy Analyst Review Comments:	<p>Reviewer: Nestor Villafuerte</p> <p>11/20/2025 All comments have been addressed. This PIA is ready for SAOP review and approval.</p> <p>8/13/2025 Please see comments and update accordingly:</p> <p>PTA-5:</p> <p>Please add the following sentence in the beginning of your response:</p> <p>"The system will collect and maintain the following PII elements:"</p> <p>Also, please write out "TIN", "NPI" and "DBA" on their first instance.</p> <p>PIA-22: Please include the provider address as mentio</p>	# of Days - APA Review:	36

SAOP Review

SAOP Review Decision:	Approved	SAOP Review Date:	11/20/2025
SAOP Review Comments:		# of Days - SAOP Review:	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
11/20/2025 10:59 AM	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 20A	VILLAFUERTE, NESTOR	10/15/2025	Question for HHS - Is there an HHS TPWA in place for ReCAPTCHA? If not, we can initiate one through the HSDW form.	
PTA 20A	VILLAFUERTE, NESTOR	10/15/2025	Question for HHS - Is there an HHS TPWA in place for ReCAPTCHA? If not, we can initiate one through the HSDW form.	
PTA 20A	BLAND, CRYSTAL	10/15/2025	Question for HHS - Is there an HHS TPWA in place for ReCAPTCHA? If not, we can initiate one through the HSDW form.	HRSA - SF - PRF - QTR2 - 2024 - HRSA1360544_09182024 Approved.rtf
PTA 20A	BLAND, CRYSTAL	10/15/2025	Question for HHS - Is there an HHS TPWA in place for ReCAPTCHA? If not, we can initiate one through the HSDW form.	