Privacy Impact Assessment (PIA): HRSA - SF - PRF - QTR1 - 2021 - HRSA701977

Date Signed: 3/2/2021

**Acronyms**

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

## General Information

| | | | |
|---|---|---|---|
| **Status:** | Approved | | |
| **PIA ID:** | 1296294 | | |
| **PIA Name:** | HRSA - SF - PRF - QTR1 - 2021 - HRSA701977 | **Title:** | HRSA - CARES Provider Relief Fund Payment Portal |
| **OpDIV:** | HRSA | | |

## PTA

| | | |
|---|---|---|
| **PTA - 1A:** | Identify the Enterprise Performance Lifecycle Phase of the system | Initiation |
| **PTA - 1B:** | Is this a FISMA-Reportable system? | Yes |
| **PTA - 2:** | Does the system include a website or online application? | No |
| **PTA - 3:** | Is the system or electronic collection, agency or contractor operated? | Agency |
| **PTA - 3A:** | Is the data contained in the system owned by the agency or contractor? | Agency |
| **PTA - 5:** | Does the system have or is it covered by a Security Authorization to Operate (ATO)? | No |
| **PTA - 5B:** | If no, Planned Date of ATO | 12/15/2020 |
| **PTA - 6:** | Indicate the following reason(s) for this PTA. Choose from the following options. | New |

| | | |
|---|---|---|
| **PTA - 8:** | Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions? | 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<br>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 |
| **PTA - 9:** | List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored. | Provider Identity Information<br>TIN<br>NPI<br>Provider Type<br>Business Name, DBA<br>Provider Address (HQ)<br>Street 1<br>Street 2<br>City<br>State<br>Zip<br>Filing Contact Identify<br>Filing Contact Name<br>Filing Contact Title<br>Filing Contact Phone Number<br>Filing Contact Email<br>Display Acquisition/Divestiture information pulled from profile<br>Display Subsidiary TINs that provider will be reporting on from profile.<br>Ask provider if Parent will be reporting on the General Distribution on their behalf.<br>PRF Amount Received<br>Display Payments to Provider<br>Additional Provider Payment Information<br>Financial Information: Un-reimbursed Expenses<br>Financial Information: Lost Revenues Attributable to Coronavirus<br>Patient Metrics<br>Facility Metrics<br>Survey Questions<br>User Access Information<br>Internal HRSA staff will be validated through AMS<br>Providers will use email and password with multi-factor authentication through Salesforce mobile app Authenticator for verification. |
| **PTA - 9A:** | Are user credentials used to access the system? | Yes |
| **PTA - 9B:** | Please identify the type of user credentials used to access the system. | HHS User Credentials<br>HHS/OpDiv PIV Card<br>Non-HHS User Credentials<br>Password<br>Username |
| **PTA - 10:** | Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should 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. 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 - 10A:** | Are records in the system | Yes |

| | | |
|---|---|---|
| | retrieved by one or more PII data elements? | |
| **PTA - 10B:** | Please specify which PII data elements are used. | Name, E-Mail, Phone Number, Taxpayer ID, Mailing Address, Financial account info, employment status |
| **PTA - 11:** | Does the system collect, maintain, use or share PII? | Yes |

## PIA

| | | |
|---|---|---|
| **PIA - 1:** | Indicate the type of PII that the system will collect or maintain | Name<br>E-Mail Address<br>Phone numbers<br>Taxpayer ID<br>Mailing Address<br>Financial Account Info<br>Employment Status |
| **PIA - 2:** | Indicate the categories of individuals about whom PII is collected, maintained or shared | Employees/ HHS Direct Contractors<br>Public Citizens<br>Other |
| **PIA - 3:** | Indicate the approximate number of individuals whose PII is maintained in the system | Above 2000 |
| **PIA - 4:** | 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 - 5:** | 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 - 6:** | Describe the function of the SSN/Taxpayer ID. | The social security number (SSN) is not being collected in this system.<br>Tax identification number (TIN) is required to access the system and for the disbursement of the federal funds users are requesting. |
| **PIA - 6A:** | Cite the legal authority to use the SSN | SSN is not used. |
| **PIA - 7:** | Identify legal authorities, governing information use and disclosure specific to the system and program | 5 U.S. Code (USC) 301, Departmental regulations. |
| **PIA - 8:** | 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. | A System of Records Notice (SORN) is required for the SFPRF system and is in progress. |

| | | |
|---|---|---|
| **PIA - 9:** | Identify the sources of PII in the system | Directly from an individual about whom the information pertains<br>Online<br>Government Sources<br>Within the OPDIV<br>Non-Government Sources<br>Other |
| **PIA - 9A:** | Identify the OMB information collection approval number or explain why it is not applicable. | 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 - 9B:** | Identify the OMB information collection expiration date. | |
| **PIA - 10:** | Is the PII shared with other organizations outside the system's Operating Division? | No |
| **PIA - 11:** | Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason | A warning banner with terms and conditions notice will be displayed prior to individual user's login. |
| **PIA - 12:** | Is the submission of PII by individuals voluntary or mandatory? | Mandatory |
| **PIA - 12A:** | If mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties | The Coronavirus Aid, Relief, and Economic Security Act (CARES) Act (P.L. 116-136) and the Paycheck Protection Program and Health Care Enhancement Act (P.L. 116-139) appropriated funds to reimburse eligible healthcare providers for healthcare related expenses or lost revenues attributable to the coronavirus. These funds were distributed through the CARES Act Provider Relief Fund (PRF) program. Recipients of these funds agreed to Terms & Conditions which require compliance with reporting requirements, including providing PII. |
| **PIA - 13:** | 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 | 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 - 14:** | 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). Alternatively, describe why they cannot be notified or have their consent obtained | 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 - 15:** | 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 | 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. |

| | | |
|---|---|---|
| | PII is inaccurate. If no process exists, explain why not | |
| **PIA - 16:** | Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. 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 - 17:** | Identify who will have access to the PII in the system and the reason why they require access | Users<br>Administrators<br>Developers<br>Contractors |
| **PIA - 17A:** | Provide the reason of access for each of the groups identified in PIA -17 | Users: Users have access to only their own PII and those of their subsidiaries.<br>Administrators: Admins are granted access for maintenance of the system.<br>Developers: Only select developers with HRSA government furnished equipment (GFE) and access will have to use PII for prepare for user acceptance testing (UAT).<br>Contractors: Direct Contractors with HRSA with personal identity verification (PIV)/Government furnished equipment(GFE) for development and operations of the system |
| **PIA - 17B:** | Select the type of contractor | HHS/OpDiv Direct Contractor |
| **PIA - 18:** | Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII | Need to complete privacy 101, cyber security training and also complete rules of behavior (ROB) / non-disclosure agreement (NDA) |
| **PIA - 19:** | Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job | All system users with access to the production environment will have read access to PII. **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. |
| **PIA - 20:** | 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 | All HRSA employees and direct contractors that use the HRSA PRF are required to take government-furnished annual security awareness training.<br>All system users will receive system training and HRSA PRF user guides to support the various functions of the system.<br>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. |
| **PIA - 21:** | Describe training system users receive (above and beyond general security and privacy awareness training). | There is no additional formal training provided by HRSA. |
| **PIA - 23:** | Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific 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. |
| **PIA - 24:** | 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.<br>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.<br><br>Technical controls<br>Transport Layer Security (TLS) 1.2 or higher is being used for its Hypertext Transfer Protocol Secure (HTTPS) connections.; two-factor authentication; logical access controls; anti-virus software; firewalls; and role-based access<br>Data is contained in Salesforce Federal Risk and Authorization Management Program (FedRAMP) Gov Cloud. Password complexity: Length at least 8 characters; password cannot contain first name or last name; password must contain at least three of these four-character types: Uppercase, Lowercase, Numbers, or Special Character; last 6 passwords cannot be repeated and password clipping levels established to lock accounts for 15 minutes that use incorrect password more than 5 times.<br><br>Physical controls<br>The HRSA PRF system is hosted in the Salesforce FedRAMP Gov Cloud so all physical controls are implemented by the Salesforce FedRAMP authority to operate (ATO) |