

Date Signed: 5/21/2021

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

PIA ID: 1329193

PIA Name:	HRSA - PRF DMACS - QTR2 - 2021 - HRSA739926	Title:	HRSA - CARES Provider Relief Fund Payment Portal
------------------	---	---------------	--

OpDiv: HRSA

PTA

PTA - 1A: Identify the Enterprise Performance Lifecycle Phase of the system Development

PTA - 1B: Is this a FISMA-Reportable system? No

PTA - 2: Does the system include a website or online application? Yes

URL Details

Type of URL	List Of URL
HHS Intranet (HHS Internal)	https://prfdashboards.hrsa.gov

HHS Intranet (HHS Internal)	https://prfdashboards.hrsa.gov
-----------------------------	---

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 No

	by a Security Authorization to Operate (ATO)?	
PTA - 5B:	If no, Planned Date of ATO	4/30/2021
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?	<p>The purpose of Enterprise Data Mart and Analytics Cloud Pilot is to modernize the on-premises Data Mart solution to meet the functional and technical requirements of the rapidly growing and evolving HRSA programs.</p> <p>The current solution has a limitation in storage scalability to meet the future needs of HRSA. As a result, the Enterprise DataMart and Analytics Cloud solution has been identified to provide On-demand scalability, high performance and cost saving solution to meet future needs of HRSA higher analytical and visualization demand.</p>
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.	<p>The information is collected from various HRSA sources and stored in snowflake for reporting, tracking and analyses purpose.</p> <p>This information will be stored in accordance with HRSA guidelines for records management.</p> <p>Following information will be collected</p> <ul style="list-style-type: none"> Provider Identity Information TIN NPI Provider Type Business Name, DBA Provider Address (HQ) <ul style="list-style-type: none"> Street City State Zip Filing Contact Identify, Name, Title, Phone Number, Email Subsidiary TINs PRF Amount and additional Provider Payment Information Financial Transactions Data Patient Metrics Facility Metrics DocuSign Envelope IDs PRF Submission data User Access Information PRF Inquiries data Banking information Records of funds disbursed Record of attestation

Vaccination data

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

HHS Password

HHS Username

HHS/OpDiv PIV Card

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 collects the user's identity information which is used to identify the individual for various initiative to support HRSA COVID Provider Relief, Bureau vaccination and other HRSA programs. The data in the system includes PII elements such as TIN, Demographic information, Email address etc. The information is collected from various HRSA sources and stored in snowflake for reporting, tracking and analyses purpose. This information is also viable to evaluating the use of emergency government funding for future pandemics and other initiatives within HRSA. The system also collects all inquiry information to address any issues or technical challenges the users may have during their reporting. All information is captured and stored in Snowflake within the boundary of the Government Cloud. This information is stored in accordance with HRSA guidelines for records management.

PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	Yes
PTA - 10B:	Please specify which PII data elements are used.	Name, E-Mail, Phone Number, Taxpayer ID, Mailing Address, Financial account information, vaccination data, health records
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	<p>E-Mail Address</p> <p>Phone numbers</p> <p>Taxpayer ID</p> <p>Mailing Address</p> <p>Financial Account Info</p> <p>Others – NPI, Provider Type, Business Name, DBA, Provider Address (HQ), Zip Code, Filing Contact Identify, Name, Title, Phone Number, Email, Subsidiary TINs, PRF Amount and additional Provider Payment Information, Financial Transactions Data, Patient Metrics, Facility Metrics, DocuSign Envelope IDs, PRF Submission data, User Access Information, PRF Inquiries data, Banking information, Records of funds disbursed, Record of attestation, Vaccination data</p>
PIA - 2:	Indicate the categories of individuals about whom PII is collected.	<p>Public Citizens</p> <p>Other</p>
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Above 2000

<p>PIA - 4:</p>	<p>For what primary purpose is the PII used?</p>	<p>The system collects the user's identity information which is used to identify the individual for various initiative to support HRSA COVID Provider Relief, Bureau vaccination and other HRSA programs. The data in the system includes PII elements such as TIN, Demographic information, Email address etc. The information is collected from various HHS/HRSA sources and stored in snowflake for reporting, tracking and analyses purpose. This information is also viable to evaluating the use of emergency government funding for future pandemics and other initiatives within HRSA. The system also collects all inquiry information to address any issues or technical challenges the users may have during their reporting. All information is captured and stored in Snowflake within the boundary of the Government Cloud. This information is stored in accordance with HRSA guidelines for records management.</p>
<p>PIA - 5:</p>	<p>Describe any secondary uses for which the PII will be used (e.g. testing, training or research)</p>	<p>PII data use for testing is masked and anonymized before moving to the testing environment.</p>
<p>PIA - 6:</p>	<p>Describe the function of the SSN/Taxpayer ID.</p>	<p>The system collects the user's identity information which is used to identify the individual for various initiative to support HRSA COVID Provider Relief, Bureau vaccination and other HRSA programs . The information is collected from various HHS/HRSA sources and stored in snowflake for reporting, tracking and analyses purpose. This information is also viable to evaluating the use of emergency government funding for future pandemics and other initiatives within HRSA.</p>
<p>PIA - 8:</p>	<p>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.</p>	<p>Snowflake is the system of record. A new SORN is under development</p>
<p>PIA - 9:</p>	<p>Identify the sources of PII in the system</p>	<p>Government Sources Within the OPDIV Non-Government Sources Other</p>
<p>PIA - 10:</p>	<p>Is the PII shared with other organizations outside the system's Operating Division?</p>	<p>No</p>
<p>PIA - 12:</p>	<p>Is the submission of PII by individuals voluntary or mandatory?</p>	<p>Voluntary</p>

<p>PIA - 16:</p>	<p>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</p>	<p>Periodic review of PII are conducted in source systems and snowflake data is refreshed every day.</p> <p>Snowflake FedRAMP solution addresses data's integrity, availability, accuracy and relevancy.</p>
<p>PIA - 17:</p>	<p>Identify who will have access to the PII in the system and the reason why they require access</p>	<p>Users</p> <p>Administrators</p> <p>Developers</p> <p>Contractors</p>
<p>PIA - 17A:</p>		<p>Provide the reason of access for each of the groups identified in PIA-17</p> <p>Users : Use reports / dashboards assigned to them which have PII.</p> <p>Administrators: Complete access to the system for management and support.</p> <p>Developers: Selected developers with HRSA GFE create reports / dashboards for the users</p> <p>Contractors: Direct Contractors with HRSA and with PIV/Government furnished equipment(GFE) for development and operations of the system</p>
<p>PIA - 17B:</p>	<p>Select the type of contractor</p>	<p>HHS/OpDiv Direct Contractor</p>
<p>PIA - 18:</p>	<p>Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII</p>	<p>HRSA bureau office determines the users who need access to DMACS and a request is sent to the OIT office for approval. Upon approval, the request is sent to DMACS Administrator, who will then create these user accounts.</p> <p>Users : Use reports / dashboards assigned to them which have PII.</p> <p>Administrators: Complete access to the system for management and support.</p> <p>Developers: Selected developers with HRSA GFE create reports / dashboards for the users</p> <p>Contractors: Direct Contractors with HRSA and with PIV/Government furnished equipment(GFE) for development and operations of the system</p>
<p>PIA - 19:</p>	<p>Describe the technical methods in place to allow those</p>	<p>DMACS establishes user access through RBAC. RBAC enforces the principle of least privileges which grant users just enough permissions needed to perform their business functions.</p>

with access to PII to only access the minimum amount of information necessary to perform their job

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 security awareness training. All system users will receive system training and HRSA PRF user guides to support the various functions of the system. 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 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 except for Significant user training provided to system administrators.

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)

DMACS 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 DMACS 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 DMACS 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.
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.

Technical controls
TLS1.2 or higher is being used for its HTTPS connections.; two-factor authentication; logical access controls; anti-virus software; firewalls; and role-based access Data is contained in Snowflake 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.

Physical controls

DataMart and Analytics Data is hosted in the Snowflake FedRAMP Gov Cloud so all physical controls are implemented by the Snowflake FedRAMP ATO. Tableau servers are provisioned within HRSA datacenter and all physical controls are covered by HRSA GSS.

PIA - 25:	Describe the purpose of the web site, 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	Purpose of the website is to leverage snowflake to store HRSA program data, and tableau to support reporting, data analytics, and data visualization for HRSA initiatives All HRSA identified / approved organizational users will have access to the website. Users will access the website through a HRSA provided internal URL
PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	No
PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	No