Privacy Impact Assessment (PIA): HRSA - HEEDC - QTR2 - 2021 - HRSA731534

Date Signed: 8/30/2021

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:	1345058		
PIA Name:	HRSA - HEEDC - QTR2 - 2021 - HRSA731534	**Title:**	HRSA - HRSA Enterprise Erwin Data Catalog
OpDIV:	HRSA		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	No
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)?	Yes
PTA - 5A:	If yes, Date of Authorization	6/22/2021
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	This is a new PTA
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?	HRSA Enterprise Erwin Data Catalog (HEEDC) organizes the technical details around data assets, or metadata, into defined, meaningful and

		searchable business assets to enable consistent understanding among all data consumers. It establishes enterprise-wide data definitions and transparency, business users can easily communicate and ensure they are using the right data, at the right time for the correct purpose. It will enable users to scan, catalog, enrich, expose, and ultimately operationalize the metadata. The solution should give the metadata context and accessibility, with the ability to incorporate Custom attributes and business meaning via the Business Glossary.
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.	User Credentials: Stored for as long as the user needs to access the system First Name Last Name Email Address Schema Names Table Names Column Names Data Types
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
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	User Credentials: This includes First name, Last name, email address which use to create a local account for the user to access system. This user account is used exclusively for system identification and authorization Schema Names, Table Names, Column Names, and Data Types: This information is collected to organizes the technical details around data assets, or metadata, into defined, meaningful and searchable business assets to enable consistent understanding among all data consumers.
PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	No
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 E-Mail Address User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Other
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Below 50
PIA - 4:	For what primary purpose is the PII used?	User credentials are created / maintained for users who need access to the system. User credentials enable users to log into the system.

PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	5 U.S.C. 301 Departmental Regulation legal authority for collecting PII (user credentials).
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Other
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	Not Applicable. User credentials are created / maintained for users who have access to the system.
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17 Users need credentials to access the system Administrators need access to manage users & user credentials Contractors need access to setup and configure 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	System owners identify the administrator who can manage / administer the system. User credentials are only granted to a few selected users based on their business function and need to know.
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	System owners identify the administrator who can manage / administer the system. User credentials are only granted to a few selected users based on their business function and need to know.
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 Enterprise Erwin Data Catalog (HEEDC) are required to take government-furnished annual security awareness training.

		All system users will receive system training and HEEDC user guides to support the various functions of the system. All HRSA employees and direct contractors that use the HEEDC System are required to take government-furnished annual security awareness trainings. Upon accessing the initial HEEDC 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 HEEDC System user acknowledges that they have completed the requisite privacy trainings, they will then be able to access the HEEDC System training materials which will in turn give them access to the HEEDC System. Without completing the privacy training acknowledgment, HEEDC 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 - 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 is implemented in HEEDC 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 HEEDC is hosted in the HRSA datacenter, and all physical controls are covered by the HRSA General Support System Authority To Operate (GSS ATO).