PTA / PIA: HRSA - JIRA - QTR3 - 2025 - HRSA1446060

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

General Information

PTA / PIA Name:	HRSA - JIRA - QTR3 - 2025 - HRSA1446060	**PTA / PIA ID:**	3913428
Component Name:	HRSA - JIRA	**ATO Boundary Name:**	JIRA
Overall Status:	Complete	**# of Days - Open:**	258
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.	7/16/2024
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	Rebecca Andam Michael Makinde
PTA 01A:	POC Title and Organization	ISSO, HRSA
PTA 01B:	POC Email Address	randam@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 PTA/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.	JIRA is a proprietary issue tracking product, developed by Atlassian to provide bug tracking, issue tracking, and project management functions. System will allow the users to create tickets for the Change requests and routes the requests to various transition steps and enables the privileged users to approve, reject, close the requests. Each of the transition step is tied up to a user group. Security in the system is tied up to JIRA User Groups and each group is provided with some actions as defined in the workflow. JIRA Authentication is synchronized with HRSA Active Directory and the directory synchronization process runs every hours. We are not using local JIRA user accounts. All users will use their HRSA Active Directory Account to login to the system. There is no direct connection of JIRA Change Request system with any applications within Division of Enterprise Solutions and Applications Management (DESAM). This system manages the Change Requests (CR) and defects to applications like Electronic Handbooks (EHB), Division of Infrastructure Support (DIS), Custom Applications Branch (CAB), HRSA Data Warehouse (HDW) and other Bureau applications that need Government approval.
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 information collected are the change requests specific to bureaus and offices. System will capture the comments/actions performed at each transition step in the workflow and display to users. JIRA Collects the User's Principal Name (UPN), Email, First and Last Name of users as part of the Directory Synchronization. This information is made available in the user management section of JIRA. User Management feature is only available to JIRA Administrator group.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card
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.	Change management systems for Electronic Handbooks (EHB). The information collected are the change requests specific to bureaus and offices. System will capture the comments/actions performed at each transition step in the workflow and display to users. The User credentials are not shared with the general public or other Government agencies. They are used to access JIRA system.
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).	Prod: https://jira.hrsa.gov QA: https://jira.test.hrsa.gov Staging: https://jira.stg.hrsa.gov
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No
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.	JIRA is a proprietary issue tracking product, developed by Atlassian to provide bug tracking, issue tracking, and project management functions. System will allow the users to create tickets for the Change requests and routes the requests to various transition steps and enables the privileged users to approve, reject, close the requests. Each of the transition step is tied up to a user group. Security in the system is tied up to JIRA User Groups and each group is provided with some actions as defined in the workflow. JIRA Authentication is synchronized with HRSA Active Directory and the directory synchronization process runs every hours. We are not using local JIRA user accounts. All users will use their HRSA Active Directory Account to login to the system. There is no direct connection of JIRA Change Request system with any applications within Division of Enterprise Solutions and Applications Management (DESAM). This system manages the Change Requests (CR) and defects to applications like Electronic Handbooks (EHB), Division of Infrastructure Support (DIS), Custom Applications Branch (CAB), HRSA Data Warehouse (HDW) and other Bureau applications that need Government approval.
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.	Biographical Information Name User Credentials Contact Information Email Address (Business) Other Other
PIA 22A:	Identify the "other" type(s) of personally identifiable information (PII) not mentioned in the above list.	User Principal Name (UPN)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors 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.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	For user authentication to JIRA System. JIRA administrators will be able to add a user to their respective JIRA Groups to provision access to JIRA Change Request (CR) System. It is also used to contact users.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	NA. JIRA does not use PII for any secondary use.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 USC 301, Departmental Regulations.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Government Sources Within the 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.	JIRA does not collect any data from individuals. JIRA is used to track projects.
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.	There is no option to opt out of providing name and email to JIRA. These are required elements to qualify one to create a tickets that provide bug tracking, issue tracking, and project management functions.
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.	No process exist because data is extracted from Active Directory.

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.	No process exist because data is extracted from Active Directory.
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.	The accuracy of the PII is validated during the data extraction from Active Directory.
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.	Administrators Reasoning: Maintain and support the database. Contractors Reasoning: Maintain, support, validate and verify the system. Users Reasoning: For search purposes
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	A user submits a request for system access to the system administrator. The administrator makes a determination as to what PII data the user has access to based on their job title and role.
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.	The system is role based and user can only access data based on their business or job needs.
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.	HRSA provides mandatory security training to all users.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	NA
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).	The process and guidelines in place with regard to the retention and destruction of PII follow the National Archives and Records Administration (NARA) General Records Schedule (GRS) 6.1, requiring all records to automatically be deleted after 6 years.

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.	HRSA takes all possible safeguards to protect data that is submitted through JIRA and to ensure that data cannot be accessed by unauthorized users. Once data is submitted through the JIRA system, the data is protected by firewalls and all JIRA servers are located in the HRSA domain. The HRSA Security Operation center constantly scan the JIRA and servers for any intrusions. All users connect to the JIRA using secure Transmission Control Protocol (TCP) port 443. JIRA users have no direct access to the backend databases. Lastly, the JIRA requires complex passwords and frequent renewal of user passwords.

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) have been addressed. This PIA is ready for SAOP review and approval. Reviewer: Nestor Villafuerte 12/12/2025 Please see comments and update accordingly: PIA-22: Please include UPN in the "other" section per PTA5. PIA-44: Record schedule 25 was superseded and replace with GRS 6.1.	**# 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 3:41 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
PIA 22A	VILLAFUERTE, NESTOR	12/15/2025	Added User Principal Name (UPN) to other	
PIA 22A	BLAND, CRYSTAL	12/15/2025	Added User Principal Name (UPN) to other	