Privacy Impact Assessment (PIA): HRSA - JIRA - QTR3 - 2020 - HRSA610687

Signed Date: 9/16/2020

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:	1185185
PIA Name:	HRSA - JIRA - QTR3 - 2020 - HRSA610687	**Title:**	HRSA - JIRA
OpDiv :	HRSA		
Legacy PIA ID:			

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	Yes
PTA - 2:	Does the system include a website or online application?	No
PTA - 2A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	

URL Details

Type of URL	List Of URL
No Records Found	

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?	
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	7/30/2018
PTA - 5B:	If no, Planned Date of ATO	8/2/2017
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?	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 - 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.	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 -9A:	Are user credentials used to access the system?	
PTA - 9B:	Please identify the type of user credentials used to access the system.	HHS User Credentials 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	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 - 10A:	Are records in the system retrieved by one or more PII data elements?	No
PTA - 10B:	Please specify which PII data elements are used.	
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
PIA - 2:	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 - 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?	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 - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	NA
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	5 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.	NA
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Email Government Sources Within the OPDIV Non-Government Sources Other
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	Data that JIRA CR System is using is not collected from any website. Data is directly synchronized using HRSA Lightweight Directory Access Protocol (LDAP)/Active Directory (AD) connector. The PII collected are only used for access and maintaining contact. User credentials are also used for access.
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	Data that is being synchronized for JIRA system authentication purposes is already available in HRSA Global Address List.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
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	There is no option to opt out of providing name and email to JIRA. These are required elements to qualify one to create a ticket that provide bug tracking, issue tracking, and project management functions.
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	JIRA notifies the user that they are accessing a federal system each time they attempt to access the system. However, when the JIRA implements changes to the system that enhances functionality, the PII is not affected. Users can still access the system using their credentials. Anytime a user accepts the system notification use, provides consent to the JIRA to changes to the system without further notification to the end user.
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 PII is inaccurate. If no process exists, explain why not	In the event that PII or user credentials is inappropriately obtained, used or disclosed the Network Operations Center (NOC) will notify the Information System Security Officer and

		Contracting Officer Representative (COR) . The COR will then send an email to the affected party to inform them about the incident.
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	JIRA implements a network and host-based Intrusion Detection System (IDS) It also uses audit technology to track changes to the application and its data. The (Network Operations Center) NOC reviews the IDS logs weekly for anomalies and the Database Administrators review the audit logs quarterly to ensure the integrity, availability, accuracy and relevancy of the data. The end users at a minimum access their information annually using their credentials to assess and evaluate their stored information.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17	Administrators Reasoning: Maintain and support the database. Developers Reasoning: Validate and verify system changes Contractors Reasoning: Maintain, support, validate and verify 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	The users (administrators, developers, and contractors) are vetted through the HRSA background investigation process. Once they have been cleared through that process, the HRSA Contracting Officer Representative (COR) authorizes and approves request for access from the contractor. The users receive access to the system for the sole purpose of performance monitoring, data maintenance and account management.
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	The system is role based and user can only access data based on their business or job needs.
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	HRSA provides mandatory security training to all users.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	NA
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)	Only active users from HRSA Active directory are used for synchronization. Data Sync job runs twice a day to update the AD Users information. The JIRA system currently retains PII for only as long as necessary to fulfill the specified purpose(s). User credentials are disabled and removed after 18 months of inactivity. We are working with HRSA's Records Management Office, who are in turn working with National Archives and Records Administration (NARA) to obtain the appropriate records and retention schedule.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address	HRSA takes all possible safeguards to protect data that is submitted through JIRA and to ensure

	each element in your response	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 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.
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	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.
PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	No
PIA - 27A:	Select the type of website measurement and customization technologies is in use and if it is used to collect PII	
PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No
PIA - 28B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	No