Privacy Impact Assessment (PIA): OS - JSM - QTR3 - 2024 - OS2175233

Created Date: 8/30/2024 5:04 PM Last Updated: 2/20/2025 1:20 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

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 Name:	OS - JSM - QTR3 - 2024 - OS2175233	**PIA ID:**	2165103
Name of Component:	OS - OS - OS - ONC JIRA Service Manager	**Name of ATO Boundary:**	ONC JIRA Service Manager
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	189
Submission Status:	Submitted	**Submit Date:**	1/14/2025
Next Assessment Date:	N/A	**Expiration Date:**	2/20/2028
Office:		**OPDIV:**	OS
Security Categorization:	Moderate	**OpDiv PIA ID:**	OS2175233
Legacy PIA ID:		**Make PIA available to Public?:**	No

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	12/2/2022
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	No changes occurred since the last PIA.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	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 system will be used by the public to submit questions, comments, feedback and complaints about Health Information Technology (IT) vendors and certifications programs of Office of National Coordinator for Health IT (ONC).

PTA - 5:	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 following information is captured with the submission of a ticket through the Inquiry and Feedback Portal. These are consistent across all public submissions. Submitters have option to remain anonymous, but if they decline, collect First Name, Last Name, Email. Description (complaint/inquiry details – free text), Attachments (optional as relevant to issue). Issues related to health IT certification/Certification program are also asked for details on the related program condition (drop down menu) As PII is added into/grows in the data collection, we expect fields such as address, employer ID, and/or National Provider ID may also be provided to support response to submissions. **Storage**: As the inclusion of PII is new to processes, data will be stored for the foreseeable future (no specified end date) with potential to adjust as needed.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS Username Password Non-HHS User Credentials Username Password
PTA - 6:	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 following information is captured with the submission of a ticket through the Inquiry and Feedback Portal. These are consistent across all public submissions. Submitters have option to remain anonymous, but if they decline, collect First Name, Last Name, Email. Description (complaint/inquiry details – free text), Attachments (optional as relevant to issue). Issues related to health IT certification/Certification program are also asked for details on the related program condition (drop down menu) As PII is added into/grows in the data collection, we expect fields such as address, employer ID, and/or National Provider ID may also be provided in certain claims to support response to submissions

PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes
PTA - 9:	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.	The website will be used by the public to submit questions, comments, feedback and complaints about Health Information Technology (IT) vendors and certifications programs of Office of National Coordinator for Health IT (ONC).
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?	Yes
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	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?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA		
PIA		
PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Other - Free text Field - Provider Address, Employer ID, National Provider ID
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	51 - 200
PIA - 4:	For what primary purpose is the PII used?	The intent is to collect information so Office of National Coordinator for Health IT (ONC) can build cases for investigation of potential actors that may be committing information blocking. The information collected will be very detailed and specific to the actor and incident, as there are monetary penalties per incident. These are records will likely take years to investigate, especially with the likelihood of litigation.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	N/A
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	H.R.34 - 21st Century Cures Act
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	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.	
PIA - 9:	Identify the sources of PII in the system.	Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	Data collected does not reach the level of Paperwork Reduction Act (PRA) requirements.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Private Sector Within HHS

PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	For purposes of information blocking claims, the intent of these disclosures is to collect information so ONC can build cases for investigation of potential actors that may be committing information blocking. The information collected will be very detailed and specific to the actor and incident, as there are monetary penalties per incident. These are records will likely take years to investigate, especially with the likelihood of litigation. For purposes of complaints, PII is shared if the complainant provides explicit permission to share their information with the ONC- Authorized Certification Bodies (ACB) and if the health IT for which they are submitting a complaint has been identified as an active product under the ONC Health IT Certification Program. The disclosures in these instances allow for further investigation by the ONC-ACB as to the potential non-conformities for which a developer may be subject to under the ONC Health IT Certification Program.
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	N/A
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	Inclusion of PII is optional and determined by the public submitter as to its inclusion to support inquiries or complaints. Unauthorized disclosure of PII will initiate the ONC incident response process in accordance with HHS PII incident reporting process. Sharing of tickets that include PII only occurs with authorized users. PII is not disclosed or used in any other setting beyond its role in assisting response to system tickets. The only users who will have access to the PII information will ONC/HHS Staff and Audacious Inquiry Staff authorized by ONC COR. ACB and OIG users will only have access to a limited portal for tickets that are explicitly shared with them by ONC/HHS/Audacious Inquiry staff. For a new ONC/HHS/ACB/OIG user to obtain access, the COR of the project must submit a request/elevate access ticket to the system administrators. Before submitting the access request, the COR will also ensure that user has completed required trainings and has the appropriate clearance required to obtain access. For a new Audacious Inquiry staff to obtain access, the system administrators will submit formal request for approval via email and ticket to the COR. Before submitting the ticket, administrators of the system will ensure that the new staff member has completed all the required trainings and cleared the background check initiated by Audacious Inquiry's security and compliance team.

PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can 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 opt-out option for the collection or use of PII because providing PII is not required for submissions. It is entirely up to the individuals submitting a claim to determine if they need to include PII. They are not required to submit PII as a part of the inquiry/claim process.
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.	The core functionality of the system is enabled by a portal that helps users of the system submit information. During the submission process, the system will not let the users submit information to the system unless the user checks the option "I agree to the ONC's privacy policy". The words "ONC's privacy policy" is a hyperlink that directs the users to a public page that describes all the privacy, data collection and sharing policies.
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.	Unauthorized disclosure of PII will initiate the ONC incident response process in accordance with HHS PII incident reporting process.
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.	No process in place. The system is not designed to ensure the accuracy of the PII/PHI provided by individuals. There is no function for PII/PHI integrity built into the system. Individuals are responsible for ensuring the accuracy of any information submitted as a part of their claim.
PIA - 17:	Identify who will have access to the PII in the system.	Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Contractors are required to access PII for administration of the system environment and inquiries of the website.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The only users who will have access to the PII information will ONC/HHS Staff and Audacious Inquiry Staff authorized by ONC Contracting Officer's Representative (COR). For a new ONC/HHS user to obtain access, the COR of the project must submit a request/elevate access ticket to the system administrators. Before submitting the access request, the COR will also ensure that user has completed required trainings and has the appropriate clearance required to obtain access. For a new Audacious Inquiry staff to obtain access, the system administrators will submit formal request for approval via email and ticket to the COR. Before submitting the ticket, administrators of the system will ensure that the new staff member has completed all the required trainings and cleared the background check initiated by Audacious Inquiry's security and compliance team.
PIA - 20:	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 access management in the system is performed using issue security, group security and permission schemes of Jira. For the personnel needing access to PII, a detailed access request will be initiated by the COR. Based on the information provided by the approved authority, the administrators will add the new user to appropriate user group and set proper issue security schemes to allow access to only necessary information required to perform their job.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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.	Onboarding of new employees is provided as well as access to Help Guides for those interacting with the system. As updates are made, further webinar training is provided on an as-needed basis.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	ONC users and contractors do not receive any additional security or privacy training other than what's required by the ONC and HHS.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	Destruction of PII will be performed in accordance with NIST SP 800-88, Guidelines for Media Sanitization. JSM follows HHS's policy for records management, which can be found here: https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-ocio-policy-for-records-management.html. As JSM serves as a system of record, the JSM system retains all data in perpetuity, only archiving and not destroying any data in the system. General Records Schedule (GRS) 3.2 Item 030, Disposition Authority: DAA-GRS-2013-0006-0003. Destroy when business use ceases.

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**: PII policies will be outlined in help guides and training of personnel using system. New access requests to the PII will be thoroughly reviewed as per the prescribed access management policy **Technical**: The data at rest is stored in Amazon Web Service (AWS) Relational Database Service (RDS) servers. Amazon RDS servers are encrypted Database (DB) instances and use the industry standard AES-256 encryption algorithm to encrypt data on the server All the servers required for this system are hosted in AWS and data is also encrypted in transit using Transport Layer Security 1.2 (TLS) with an industry-standard AES-256 cipher. **Physical**: AWS data center physical access controls can be found at: https://aws.amazon.com/compliance/data-center/controls/

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	1/15/2025
Privacy Analyst Comments:	Vanessa, this PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	1/17/2025
		SOP Days Open:	3

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	1/24/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 1/24/2025 All comments have been addressed. This PIA is ready for SAOP review and approval. 9/3/2024 Please see comments below and update accordingly: PIA-23: Please cite specific records retention schedules. Please list any of NARA's Records Control Schedule (RCS) Job Numbers or General Records Schedules (GRSs) that apply to the PII maintained in the system; and/or State if NARA is determining the appropriate RCS Job Number or GRS for some or all the PII maintained in the system and that the PII should be maintained until a determination is provided. Since this PIA will be a public-facing document, your response to PIA-23 should include information about the records schedule that is being referenced (for example, including the number of years that the records will be retained before they are destroyed). This information will help members of the public understand how long these records are kept in the system.	**Agency Privacy Analyst Days Open:**	7

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	2/20/2025
		SAOP Days Open:	27

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 11B	Data Feed Service, piafrmos_Release	8/26/2024	ONC-Authorized Certification Bodies (ONC-ACBs)	
PIA - 11D	Data Feed Service, piafrmos_Release	8/26/2024	Contracting Officer's Representative (COR) Office of Inspector General (OIG)	

PIA - 11B	VILLAFUERTE, NESTOR	9/3/2024	Please write out acronym ONC-ACB.
PIA - 23	BLAND, CRYSTAL	9/3/2024	Please cite specific records retention schedules. Please list any of NARA's Records Control Schedule (RCS) Job Numbers or General Records Schedules (GRSs) that apply to the PII maintained in the system; and/or State if NARA is determining the appropriate RCS Job Number or GRS for some or all the PII maintained in the system and that the PII should be maintained until a determination is provided. Since this PIA will be a public-facing document, your response to PIA-23 should include information about the records schedule that is being referenced (for example, including the number of years that the records will be retained before they are destroyed). This information will help members of the public understand how long these records are kept in the system.
PIA - 23	Data Feed Service, piafrmos_Release	9/27/2024	The department would like this response to have a specific NARA GRS listed. Please list any of NARA's Records Control Schedule (RCS) Job Numbers or General Records Schedules (GRSs) that apply to the information maintained in the system; and/or State if NARA is determining the appropriate RCS Job Number or GRS for some or all of the information maintained in the system and that the PII should be maintained until a determination is provided. If you need assistance in determining this please reach out to: Karen Ballesteros and HHSRecordsManagement@hhs.gov An example of this would be the following response: "General Records Schedule (GRS) 3.2. Item 010, Disposition Authority: DAA-GRS-2013-0006-0001. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system."

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	2/20/2025 1:20 PM	**History Log:**	View History Log