Privacy Impact Assessment (PIA): CDC - CDC NAC-G - QTR2 - 2024 - CDC8283724

Created Date: 6/13/2024 4:02 PM Last Updated: 9/24/2024 12:01 AM

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:	CDC - CDC NAC-G - QTR2 - 2024 - CDC8283724	**PIA ID:**	1901561
Name of Component:	CDC - CDC Nintex Automation Cloud for Government	**Name of ATO Boundary:**	CDC Nintex Automation Cloud for Government
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	122
Submission Status:	Re-Submitted	**Submit Date:**	9/5/2024
Next Assessment Date:	N/A	**Expiration Date:**	9/23/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8283724
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	9/30/2024
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have 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.	Nintex Automation Cloud for Government (NAC-G) is a FedRAMP authorized Software as a Service (SaaS). This SaaS is the next generation upgrade of Nintex for O365 widely used at CDC to support program workflows and forms. OCIO's CDC NAC-G allows programs to automate both simple and sophisticated business processes, such as approving and signing documents, or reviewing and approving purchases. With a simple drag-and-drop, no-code interface, users can design workflows, forms and tasks, and integrate third-party platforms such as Salesforce, Microsoft Office, Office 365, SharePoint and more, and create a seamless experience that minimizes manual touchpoints and streamlines efficiency. Through Workflow Connections, the CDC controls which third-party services to connect workflows to and will know data is secure and compliant throughout the process. Nintex Forms for Office 365 and Nintex Workflow for Office 365 both have been incorporated into the CDC Office 365 system to provide customized workflows, forms, and documents that extend both the content and data being used within the environment. Nintex Automation Cloud for Government is deployed in dedicated virtual networks in the Microsoft Azure Government Virginia region (with a secondary Disaster recovery region in Azure Government Texas) within the Project Hosts' GSS One- Azure General Support System, connected via virtual network peering. The subnets dedicated to Nintex are isolated from other subnets by Azure Network Security Group access controls, and they form the boundary for the Nintex Automation Cloud for Government system. These NSG Rules are configured with the principle of least privilege and are configured in a deny all, allow by exception mannerism only allowing specific inbound and outbound traffic on specific ports to specific IP addresses or PaaS Services. The core of Nintex Automation Cloud for Government is hosted with a Kubernetes cluster running on Microsoft Azure Kubernetes Service. The Kubernetes cluster runs a collection of microservices. All data stored by the microservices is stored in Microsoft Azure PaaS, accessed via HTTPS and will be scanned according to *FedRAMP Vulnerability Scanning Requirements for the deployment and use of containers*. TLS termination is performed at the Kubernetes edge.
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 data contained and/or processed within this system is owned and used by the respective End-user / Center / Institute / Office. Data Types within the system: Goods acquisition, which involves the procurement of physical goods, products, and capital assets to be used by the Federal government.

IT Security, which involves all functions pertaining to the securing of

Federal data and systems through the creation and definition of security policies, procedures and controls covering such services as identification, authentication, and non-repudiation.

Services acquisition, which involves the oversight and/or management of contractors and service providers from the private sector.

Central Records and Statistics Management

Personal Identity and Authentication

Lifecycle/Change Management

Information Sharing

Access to Care

Population Health Management and Consumer Safety

Health Care Administration

Health Care Research and Practitioner Education

The data is collected from various sources dependent upon the End-User and/or Organization via various forms i.e. Email, Memos, Letters,

Documents, Spreadsheets, and PowerPoint Presentations.

The Workflow Engine is responsible for the execution and state-management of the workflow designs created by users. The Workflow Engine stores workflow execution and state, data submitted through forms, data sent to the workflow by third-party service events, the actions performed by the workflow, and variable values. The data stored, processed and transmitted through the component may be Federal Information such as PII depending on the workflow design. Data is stored based on the CDC Records Retention policy timeframes based on the data type.

Potential types of PII that users may elect to include: Name, Driver's License Number, Mother's Maiden name, E-Mail Address, phone numbers, medical notes, certificates, education records, military status, foreign activities, taxpayer id, date of birth, photographic identifiers, vehicle identifiers, mailing address, medical records number, financial account info, legal documents, device identifiers, employment status, or passport number. These categories only apply as a user may choose to include such information and unspecified PII in a form and/or email message, although it is not required by the information system. Active Directory credential information

		(UserID) and IP address to allow for mailbox synchronization and email delivery may also be included. Information maintained within Nintex and/or the leveraged component CDC O365 includes User identifier, first, middle and last name, organization, office number, email address, IP address, and their individual work phone number. Within the Microsoft Teams component, Equal Employment Office (EEO) legal documents will also be included. These legal documents will include complaints, settlements, alternative dispute resolution, and reasonable accommodations for CDC EEO cases. These documents may include CDC employee names, mailing address, date of birth, medical records number, financial information related settlement agreements, and employment status. Business contact information on external parties related to the cases, such as professionals (attorneys, doctors, representatives), and witnesses who may include public citizens.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	

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.	Nintex Forms for Office 365 and Nintex Workflow for Office 365 both have been incorporated into the CDC Office 365 system to provide customized workflows, forms, and documents that extend both the content and data being used within the environment. Nintex users can create and possibly send forms and workflows that could potentially contain PII via CDC O365 that stores or passes PII and any other information (text, images, uniform resource locators (URL), attachments, etc.), contained in emails between individual users sending and receiving emails on the system. Individual users control the content of messages they send and must adhere to applicable law and policy, including the Health and Human Services (HHS) Rules of Behavior when using the email service. The nature of the information transmitted will vary widely, as users work in a variety of roles and subject matter areas. Since the information is not required by the system but is incidentally collected as a result of the nature of the application, no definitive purpose can be surmised other than to meet the specific needs of the individual user/sender. User identifier, first, middle and last name, organization, office number, email address, IP address, and users individual work phone number are collected for user identification, authentication, and account maintenance. CDC employee names, mailing address, date of birth, medical records number, financial information related to settlement agreements, employment status, and business contact information for professionals are collected for legal documents related to CDC EEO cases, including complaints, settlements, alternative dispute resolutions, and reasonable accommodations.
PTA - 7:	Does the system collect, maintain, use or share PII?	
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	
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)?	No

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.	Participant users interact with Nintex Workflows via forms hosted in the web browser. Form submissions are used to start workflows or respond to workflow tasks. Forms can be configured to require user authentication, which uses the user's Nintex Automation Cloud for Government credentials with the same Okta authentication process as Designers, Administrators and Developers. Forms can also be configured to be accessed/submitted anonymously. Anonymous forms can only be accessed via a direct URL link. Authenticated forms can be accessed via a direct link or by navigating to the Participant dashboard which shows a user the tasks assigned to them and the status of forms and workflows that they have previously submitted.
PTA - 10:	Does the website have a posted privacy notice?	
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
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 Mother Maiden Name Email Address Phone numbers Medical records (PHI) Certificates Education Records Military Status Foreign Activities Date of Birth Photographic Identifiers Vehicle Identifiers Mailing Address Medical Records Number Financial Account Info Legal Documents Devices Identifiers Employment Status Passport Number User Credentials Driver License Number Other - Free text Field - Medical Notes
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Grantees Patients 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?	The data contained and/or processed within this system is owned and used by the respective End-user / Center / Institute / Office. Data Types within the system: Goods acquisition, which involves the procurement of physical goods, products, and capital assets to be used by the Federal government. IT Security, which involves all functions pertaining to the securing of federal data and systems through the creation and definition of security policies, procedures and controls covering such services as identification, authentication, and non-repudiation. Services acquisition, which involves the oversight and/or management of contractors and service providers from the private sector. Central Records and Statistics Management Personal Identity and Authentication Lifecycle/Change Management Information Sharing Access to Care Population Health Management and Consumer Safety Health Care Administration Health Care Research and Practitioner Education The data is collected from various sources dependent upon the End-User and/or Organization via various forms i.e. Email, Memos, Letters, Documents, Spreadsheets, and PowerPoint Presentations and would be used to create Workflows.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	PII is not used for any other purposes.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable. SSN/Taxpayer ID is not requested or required as part of the agency's or individuals' use of this system. SSNs may be transmitted in individual emails, but not according to any particular, defined use.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable. SSN/Taxpayer ID is not requested or required as part of the agency's or individuals' use of this system. SSNs may be transmitted in individual emails, but not according to any particular, defined use.

PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 U.S.C. 301, which provides authority for the agency to establish the organizations, procedures and tools necessary to perform its duties and pursue its mission. Information use and disclosure for this system is governed by the laws and regulations of the individual business practice that this system is used to conduct. Users work in various agency organizations that have different functions and are subject to different laws and regulations.
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.	Directly from an individual about whom the information pertains Email Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Other Federal Entities
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.	An OMB information collection approval number is not required due because the Nintex system does not promulgate a paper form, website, survey or electronic submission that will impose an information collection burden on the general public.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
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)).	
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.	
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.	The Individuals can choose not to provide PII via email since it's provided voluntarily. However, the name and email address of the users creating forms and task within Nintex are required as part of the system functionality and configuration in order to send/receive workflow task and forms.
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 system owner and/or administrator notifies the impacted individuals via mail and/or email to inform them to obtain consent regarding disclosure and/or data usage changes.
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.	The system owner, administrator and Systems Security Privacy Officer (SSPO) works together with the individual impacted to resolve any concerns when they believe their PII has been compromised by reporting an incident to the Cybersecurity Incident Response Team (CSIRT) where a ticket is created and assigned to a Security analyst to investigate and remediate in a timely manner.
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.	Data integrity is maintained at the level of the business process, or through maintenance of the applications that support business processes. The Office 365 information used by Nintex originates from a separate information system which has its own processes for maintaining integrity, availability, accuracy and relevancy. Agency-wide cybersecurity, physical security, continuing operations and other measures also support data integrity and availability and system functionality. Users are responsible for the accuracy and relevancy of PII they transmit over Nintex.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors Third-Party Contractor (Contractors other than HHS 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.	Users: To send emails, create workflows and tasks to perform duties. Administrators: As the administrator, the Xtensions Application Programming Interface (API) is responsible for managing connections to third-party services. The Xtensions API is used for Nintex-provided workflow connectors, and Nintex Xtensions extensibility framework connectors. The Nintex Xtensions framework provides the ability for Designer, Developer and Administrator users to create custom connectors to third party services from within the workflow designer. Xtensions API securely stores the authentication information for a third-party connection. Contractors: CDC Direct Contractors have access to PII to perform work duties as required and/or needed; Offsite (indirect contractors) Microsoft Cloud Service provider support personnel (system administrators) have access to PII in order to provide technical support upon CDC request.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The Enterprise Collaboration Development Services (ECDS) Team Lead will serve as the CDC customer account manager responsible for providing access to approved CDC users. The NAC-G info system automatically disables inactive accounts after ninety (90) days for user accounts. The Nintex Deployment Admin explicitly authorizes privileged access for users by requesting that Project Hosts set up role-based access and by reauthorizing that access each time it is needed for production systems and every 60 days in the test environment. Only the privileged user roles in are authorized to access information about multitenant configurations (security-relevant information). Only Server Admins have access to the security functions (Operating System Admin access) required to install software updates.
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 roles can be assigned to a user by the CDC Nintex administrator to allow them the ability to perform certain actions within the tenant. On top of the role, there is the restrictions of content within the platform where a particular asset such as a workflow, connection and data source can be configured to allow only a specific set of users or groups within the tenant to access it and perform an action, based on the role that they have. Therefore, access to PII is restricted based on the defined roles and access granted by the administrator. Users are only allowed access to PII if provided by the designer of the task and/or workflows.

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.	The CDC conducts annual Security and Privacy awareness training for every user that have access to the CDC network. This training is required for ALL new employees, contractors and fellows in order to gain access to CDC network. All personnel are required to complete annual refresher training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	All CDC users are required to complete Rules of Behavior and other annual compliance trainings as required by the CDC based on individual roles and responsibilities.
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).	Microsoft Azure manages the backup as part of its FedRAMP authorized Azure PaaS Services. Daily differential and weekly full backups are stored in geo-redundant blob storage in the primary and secondary regions and retained there for 7 days. Transaction log backups are also stored in geo-redundant blob storage in the primary and secondary regions and retained there for 7 days. Meeting the requirement to maintain three backups of Nintex information system documentation is inherited from Azure. Standard and Always-On databases are stored in Azure storage. The Azure Blueprint states Microsoft Azure synchronously replicates user level information stored in Azure storage, CosmosDB and other Azure Databases. This data is synchronously replicated locally using the EC14+4 algorithm which provides redundancy equivalent to three copies. Microsoft also ensures that three copies of information are maintained for SQL Azure. Nintex uses the Azure configuration mentioned above ensuring that three backups of information system documentation level information are retained at all times as described here: Geo-redundant storage (GRS) copies your data synchronously three times within a single physical location in the primary region using Locally Redundant Storage (LRS). It then copies your data asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times using LRS. MS Azure retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements The National Archives and Records Administration (NARA) records retention schedule(s) GRS_6.1.012 for Email and other types of electronic, according to Legal Citation Capstone Email and Electronic Messages will be deleted within three (3) years of creation.

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: PII is secured within the system through the use of administrative controls in the form of mandatory security awareness and privacy training for all users; role-based training for privileged users; personnel screening as required by CDC; completion of contractual agreements and Rules of Behavior; in accordance with applicable CDC policies. TECHNICAL CONTROLS: Technical controls applied to Nintex include continuous network/system monitoring; compliant encryption of data in transit; firewalls; and authentication where applicable. PHYSICAL CONTROLS: Physical controls include Hosting within data centers which control and monitor physical access to the system components, including visitor control and auditing of access records; and, protection of power equipment and cabling, transmission medium, output devices and use of emergency power and shutoff systems as well as fire and water damage protection.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	9/5/2024
Privacy Analyst Comments:	OpDiv Analyst: Joshua Mosios (Contractor)	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	9/10/2024
		SOP Days Open:	5

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	9/20/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 9/20/2024 Per CDC email (see supporting documentation), the system doesn't collect SSN or Taxpayer ID. All comments have been addressed, this PIA is ready for SAOP review and approval. 7/30/2024 Please see comments on the PIA and update accordingly.	**Agency Privacy Analyst Days Open:**	10

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	In the next iteration of the PTA update the following: PTA-5: Remove taxpayer Id from your response, per your email the system doesn't collect SSN or taxpayer ID.	**SAOP Review Date:**	9/23/2024
		SAOP Days Open:	3

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
CDC NAC-G - CDC8283724_PIA_PIM_CB_comments.rtf	977800	.rtf	7/30/2024 8:27 AM	0
Copy_of_ CDC NAC-G - CDC8283724 Privacy_Impact_Assessment_PIA_bl (8).rtf	255198	.rtf	7/30/2024 8:01 AM	0
RE_ Reminder_ Review Rejected PIA CDC - CDC NAC-G - QTR2 - 2024 - CDC8283724.pdf	921831	.pdf	9/20/2024 9:56 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	6/13/2024	Selected taxpayer ID, certificates, and taxpayer ID. Added medical notes to free text field.	
PIA - 7	Data Feed Service, piafrmcdc	6/13/2024	This is not a governing authority for this system. Please cite a governing authority that would apply to the purposes provided in PTA 4 and PIA 4.	
PIA - 6	Data Feed Service, piafrmcdc	6/13/2024	Taxpayer ID was included in the PTA. Please provide a brief explanation of its usage.	
PIA - 18	Data Feed Service, piafrmcdc	6/13/2024	Please define API and remove bullet points. Remember that the intended audience is not expected to have any understanding of information technology.	
PIA - 20	Data Feed Service, piafrmcdc	6/13/2024	Can remove everything but the last paragraph.	
PIA - 24	Data Feed Service, piafrmcdc	6/13/2024	Please shorten this response to provide more of a summary of each distinct type of control (technical, physical, administrative). You can remove all mention of specific software or tools used for these purposes and limit your response to the type of software or tool.	
PIA - 16	Data Feed Service, piafrmcdc	7/11/2024	Describe the process.	
PIA - 1	VILLAFUERTE, NESTOR	7/29/2024	Does the system have a planned ATO date? PTA-4 - Please define acronym PaaS, and TLS. Reviewer notes PTA-7, PTA-7a, PTA-10 failed to sync.	
PIA - 23	VILLAFUERTE, NESTOR	7/29/2024	Please remove the bullet points to ensure 508 compliance.	
PIA - 6	BLAND, CRYSTAL	7/30/2024	For individuals the Taxpayer ID is the same as the SSN. Are you certain that the SSN isn't collected, maintained, or stored in the system (i.e., legal documents, medical records, etc.)	
PIA - 6A	BLAND, CRYSTAL	7/30/2024	If SSN is collected, please provide the legal authority to use the SSN.	
PIA - 17	BLAND, CRYSTAL	7/30/2024	Per Q21, do contractors have access to the system? If so, then select "contractor."	

PIA - 18	BLAND, CRYSTAL	7/30/2024	If Contractor have access to the system, please provide reason for access.
PIA - 17	BLAND, CRYSTAL	7/30/2024	PIA-17A: If contractors have access please select "direct contractor," "third party contractor," or "both." PTA-17B: If Contractors have access to the system than this response should be "Yes."
PIA - 1	BLAND, CRYSTAL	7/30/2024	On the next iteration of the PTA, update the following: PTA-4 - Please define acronym PaaS, and TLS. Per CDC exported version of the PTA/PIA (see Supporting Documentation) we have confirm responses for the following questions: PTA-5A: The system uses CDC Active Directory for access control. PTA-7: Yes, PTA-7A: Yes, PTA-10: Yes
PIA - 18	Data Feed Service, piafrmcdc	9/5/2024	What role do direct contractors play?
PIA - 1	Data Feed Service, piafrmcdc	9/5/2024	Taxpayer ID is not included but is in the PTA. Please advise.
PIA - 1	BLAND, CRYSTAL	9/20/2024	In the next iteration of the PTA update the following: PTA-5: Remove taxpayer Id from your response, per your email the system doesn't collect SSN or taxpayer ID.

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:	9/24/2024 12:01 AM	**History Log:**	View History Log