Privacy Impact Assessment (PIA): CDC - CXOne - QTR2 - 2024 - CDC8276778

Created Date: 5/21/2024 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 - CXOne - QTR2 - 2024 - CDC8276778	**PIA ID:**	1832200
Name of Component:	CDC - NICE CXOne	**Name of ATO Boundary:**	NICE CXOne
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	131
Submission Status:	Re-Submitted	**Submit Date:**	9/4/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8276778
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.	
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.	The NICE inContact CXone (Also referred to as Third Party or 3rd Party Vendor) is a Contact Center as a Service (CCaaS) solution, reducing costs and improving the quality of contact center interactions. It provides a complete contact center solution including Automated Call Distribution (ACD), Interactive Voice Response (IVR), Computer Telephony Integration, an outbound dialer called the Personal Connection Dialer (PCD), integration tools and options, and data reporting and analytics all delivered across many connectivity options tailored to meet the customer's need.

The Third Party suite includes the following services:

Automated Call Distribution (ACD) ™: The core service that processes contacts, manages agents, and performs call handling. It resides on the file server that manages audio WAV files, call recordings, and tenant data storage, multiple media servers process the actual audio portion of a phone call, and a Structured Query Language (SQL) database engine stores and manages Automated Call Distribution configuration data, contact history, and report data. Web servers reside in a DMZ and service external tenant requests. Automated Call Distribution applications are developed in Microsoft.NET and C++, and are designed with fault tolerant features providing real-time recovery of active contacts in the event of hardware or application failure. The Automated Call Distribution platform is serviced by a Windows-based computer network which provides network resources, authentication, monitoring, management, and other services for the application and other administrative applications. Windows- based resources include Active Directory domain controllers, Kerio mail servers, and Domain Name Service (DNS) servers.

Interactive Voice Response (IVR) ™: This is a subservice of the Third Party Vendor's Automated Call Distribution platform. Utilizing the powerful scripting engine provided in the Automated Call Distribution platform, The third party vendor has developed a suite of IVR services to automate the processing of calls. This same IVR is also integrated into an agent-based call flow to maximize the features of call automation and the value of a live agent.

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 system stores recordings of telephone calls and chat transcripts for patrons seeking support from the CDC IT ServiceDesk or OHR Help Desk. The data includes names, User IDs, telephone numbers, and email addresses. The data is maintained in a secure exchange access system with the vendor for maximum of 30 days and is either downloaded to the CDC network share or deleted from the servers.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS Email Address 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.	Information on User ID and telephone number or email address is collected to verify the patron for support with the CDC IT ServiceDesk. This data is used to create a ticket in ServiceNow to track the request made by the patron. Information such as name, email, birthday, or user ID may be collected by the OHR Help Desk for patrons. This information is used to fulfill different requests to the Office of Human Resources in support of their mission.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
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)?	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 purpose of the website is to access UserHub, a web application that allows access to MAX, My Agent Experience that agents use to handle inbound/outbound calls and inbound chats and reporting. The URL is public. The agent uses a username/password combination to access the website. They must login and authenticate to access any resources.
PTA - 10:	Does the website have a posted privacy notice?	No
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?	Yes
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 Phone numbers Date of Birth User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ 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?	To identify employees/potential employees in order to address human resources needs and/or information technology needs.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Information is not used for any other purposes.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Social Security Numbers and/or Taxpayer IDs are not collected or used within the collection of customer interactions.

PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	N/A
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 USC Section 301, Departmental 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 Phone
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.	In guidance with OMB, the OHR Help Desk or CDC IT ServiceDesk only collects the minimal amount of data from a caller which is limited to name, user ID, and/or email address.
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 individual can choose not to use the services through the telephone systems. There are other methods to contact the support desks outside of phone contact. The individual can reach support via the CDC IT ServiceDesk Portal which routes support to the appropriate parties outside of the CXOne system.
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 data collected in the call recordings are deleted from the external system within 30 days. The vendor has processes in place to advise of any process changes to their customers at a timely manner.

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.	PII is contained within a recording. The recordings are only identifiable by a master contact id number and date/time of call recording. The recordings are not subject to be labeled with any PII nor can they be searched for PII data.
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.	All call recordings are deleted from the third party vendor servers. This data is not reviewed as it is only the record of the phone interaction. The collected data from the call is used in another system under another PTA/PIA.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	In accordance with administration of the overall system, the CXOne Admins have access to all recordings. Each CXOne Admin has Public Trust 5 Certification.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The system is configured for least privileged access requiring multifactor authentication and roles and permissions to access the call recordings. These roles and permissions are maintained and reviewed on a quarterly schedule.
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 system is configured for least privileged access requiring multifactor authentication and roles and permissions to access the call recordings. These roles and permissions are maintained and reviewed on a quarterly schedule.
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.	Each user of the CXOne system has completed CDC Mandated and contractor mandated Records Management training and Security Awareness Training which must be refreshed annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	There are no additional trainings as it relates to the mandated training hosted by the CDC and contractor entities.

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).	Records Association (NARA), General Records Schedule (GRS) 5.1 states that NICE will destroy/delete when business use ceases according to DAA-GRS-2016-0016-0001. The records are deleted from the vendor after 7 days and moved to CDC share drive location with least privileged access. The data shares are controlled by Security Stewards, Data Stewards, and Business Owners. Records are maintain in the share for one calendar year before they are deleted/destroyed or if determined they are no longer needed for administrative, legal, audit or other operational purposes. System Administrators review user accounts at least semi-annually to remove users who are no longer required access for business purposes.
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.	NICE is located at a secured facility. Physical controls are in place such as security guards to ensure access to the buildings is granted to only authorize individuals. Identification of personnel is checked at the facility. NICE uses the principle of least privilege as well as a role based access control to ensure system administrators are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties. The information is protected using Access Control Lists (ACLs) defined for allowing only administrator access to the PII. This access is further protected by the system controls which enforce two-factor authentication into the NICE system. Furthermore, the information is maintained in an encrypted manner by ensuring the databases are encrypted. Access is provided based on an approved request by the System Security and Privacy Officer (SSPO). Lastly, audit logs are reviewed for suspicious activity by the SSPO on regularly basis.

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:	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	9/11/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 9/11/2024 All comments have been addressed. This PIA is ready for SAOP review and approval. 8/26/2024 Per CDC request (see Supporting Documentation) this PIA is being rejected for CDC to Update the PII being collected. 7/25/2024 This PIA is ready for SAOP review and approval. Per CDC Email and exported PIA (see Supporting Documentation), CDC confirm the responses for: PTA-5A: Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is - Active Directory PTA-7: Yes	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Per CDC Email and exported PIA (see Supporting Documentation), CDC confirm the responses for: PTA-5A: Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is - Active Directory PTA-7: Yes	**SAOP Review Date:**	9/23/2024
		SAOP Days Open:	12

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
&-25-2024 EMAIL_Re_ CDC - CXOne - QTR2 - 2024 - CDC8276778.pdf	230551	.pdf	7/25/2024 11:32 AM	0
8-26-2024 EMAIL_Re_ CDC - CXOne - QTR2 - 2024 - CDC8276778.pdf	327806	.pdf	8/26/2024 10:30 AM	0
CDC-CXOne_Copy_of_Privacy_Threshold_Analysis_PTA_b (3).rtf	89229	.rtf	7/25/2024 11:21 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	5/21/2024	Please select "Social Security Numbers" and "Date of Birth"	
PIA - 6	Data Feed Service, piafrmcdc	5/21/2024	This does not match your responses in the PTA. Please advise.	
PIA - 23	Data Feed Service, piafrmcdc	5/21/2024	You don't need to cite/summarize the Federal Records Act. We just need a valid CDC records schedule citation.	
PIA - 24	Data Feed Service, piafrmcdc	5/21/2024	Please revise answer. For administrative security, please describe all the administrative procedures in place, such as training, procedures, documentation, etc. For technical security, please describe all technical procedures in place, beyond user access. How is the data secured? Are there encryption or other technologies in place to protect the data at rest and in transit? For physical security, please describe all physical procedures in place, such as physical locations, use of physical security, locks, badges, etc.	
PIA - 19	Data Feed Service, piafrmcdc	5/21/2024	Although not necessary, I advise clarifying this response in 19 and the corresponding response in 20 to distinguish between which are administrative and which are technical procedures.	
PIA - 20	Data Feed Service, piafrmcdc	5/21/2024	Although not necessary, I advise clarifying this response in 20 and the corresponding response in 19 to distinguish between which are administrative and which are technical procedures.	

PIA - 23	Data Feed Service, piafrmcdc	5/28/2024	Please provide a valid citation.
PIA - 1	Data Feed Service, piafrmcdc	5/28/2024	Please select user credentials
PIA - 7	Data Feed Service, piafrmcdc	5/28/2024	Please provide a valid, specific legal authority.
PIA - 24	Data Feed Service, piafrmcdc	5/28/2024	Please describe actual administrative and physical safeguards in use.
PIA - 7	Data Feed Service, piafrmcdc	5/29/2024	This is legal guidance and not considered a legal authority. A legal authority is a statute or executive order.
PIA - 23	Data Feed Service, piafrmcdc	5/29/2024	There is no valid citation here. You can cite either the General Records Schedule (GRS) found here The General Records Schedule Transmittal 34 (archives.gov) or the CDC Records Control Schedule (RCS) found here Records Control Schedules | National Archives .
PIA - 24	Data Feed Service, piafrmcdc	5/29/2024	Re-organized answer by category. However, the roles and permissions to control physical access would be a technical safeguard, not a physical safeguard. Examples of physical safeguards are locked doors, security guards, closed circuit television (CCTV), etc. Please include the relevant ones here.
PIA - 13	Data Feed Service, piafrmcdc	7/10/2024	What is the method to opt out?
PIA - 22	Data Feed Service, piafrmcdc	7/10/2024	It's not clear if this is different from the training mentioned in 21. If not please remove.
PIA - 24	Data Feed Service, piafrmcdc	7/10/2024	Describe the three controls in three separate paragraphs.
PIA - 1	BLAND, CRYSTAL	7/25/2024	On the next iteration of the PTA please update the following: PTA-5A: Provide a response as it is currently blank. PTA-7A: Currently displays as "Error" in the OIS instance of Archer.

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