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 - OCIO Azure GSS - QTR2 - 2023 - CDC6758584	**PIA ID:**	6758584
Name of Component:	OCIO Azure GSS	**Name of ATO Boundary:**	OCIO Azure GSS

Sub-Component

Software Name

No Records Found

Overall Status:	✅	**PIA Queue:**	
Submitter:	BROWN, Lashell SIZEMORE, Curtis	**# Days Open:**	94
Submission Status:	Re-Submitted	**Submit Date:**	8/23/2023
Next Assessment Date:	08/24/2026	**Expiration Date:**	8/24/2026
Office:	OD	**OpDiv:**	CDC
Security Categorization:	High		
Legacy PIA ID:		**Make PIA available to Public?:**	Yes
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		9/7/2023

Privacy Threshold Analysis (PTA)

PTA Name

CDC - OCIO Azure GSS - QTR2 - 2023 - CDC6742898

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.	Change in system name from AHB to OCIO GSS
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Contractor

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 purpose of Office of Chief Information Officer (OCIO) Azure General Support System (GSS) system is to acquire remote cloud infrastructure resources from Microsoft Azure Services. This allows the Digital Services Office (DSO) to provide Center for Disease Control and Prevention (CDC) cloud service offerings along with current services offerings to CDC customers. Microsoft Azure has Federal Risk and Authorization Management Program (FedRAMP) authority to operate a Health & Human Services (HHS) Authorization to Operate (ATO). The type of data would include Name, Date of Birth, Driver's License Number Mother's Maiden Name E-mail Address, Home Address, Phone Numbers, Medical Notes Financial Account Info, Education, Military Status and Employment Status. Data will be stored temporarily. The OCIO Azure GSS system does not collect, maintain or share user credentials. The OCIO Azure GSS relies on Active Directory user IDs, Personal Identity Verification (PIV) smart cards, and Alternate Personal Identity Verification (ALT) smart cards for access but authentication credentials are not stored as part of the OCIO Azure GSS. The Infrastructure Services Branch hosts the customers applications but does not own the data or have control over the use of the data in these systems.
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 will contain Life cycle/Change Management, System Maintenance, and Information Technology (IT) Infrastructure Maintenance Information in support of the Infrastructure Services Branch managed systems hosted within the cloud providers environment. The type of data would include Name, Date of Birth, Driver's License Number Mother's Maiden Name E-mail Address, Home Address, Phone Numbers, Medical Notes Financial Account Info, Education, Military Status and Employment Status. The data will be stored temporarily. The OCIO Azure GSS system does not collect, maintain or share user credentials. The OCIO Azure GSS system relies on Active Directory user IDs, Personal Identity Verification smart cards, and Alternate Personal Identity Verification smart cards for access but authentication credentials are not stored as part of the OCIO Azure GSS system. The Infrastructure Services Branch hosts the customers applications but does not own the data or have control over the use of the data in these systems internal users will use their CDC Active Directory credentials to access the system which are stored temporarily.
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.	The OCIO Azure General Support Systems GSS system will contain Life cycle/Change Management, System Maintenance, and IT Infrastructure Maintenance Information in support of The Infrastructure Services Branch managed systems hosted within the cloud providers environment. The type of data would include Name, Date of Birth,

Driver's License Number Mother's Maiden Name E-mail Address, Home Address, Phone Numbers, Medical Notes Financial Account Info, Education, Military Status and Employment Status. This data is used for research/analysis and to build cohorts for data analysis but will not be used to query on or for individuals. For example, fields like DOB will be used to derive an Age value which will be used to bucket employees into age bracket for analysis on the group as a whole. Data will be stored temporarily. The OCIO Azure GSS system does not collect, maintain or share user credentials. The OCIO Azure GSS relies on Active Directory user IDs, Personal Identity Verification smart cards, and Alternate Personal Identity Verification smart cards for access but authentication credentials are not stored as part of the OCIO Azure GSS system. Azure Government is a government-community cloud that offers hyper-scale compute, storage, networking, and identity management services, with world-class security. A physically and network-isolated instance of Microsoft Azure, operated by screened U.S. citizens, Azure Government provides standards-compliant Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) that has now received a Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) Provisional Authorization To Operate (ATO). All services are available immediately for supporting secure US government workloads, including Criminal Justice Information Services (CJIS), Internal Revenue Services (IRS) Publication 1075 Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA), Department of Defense (DOD), and federal agency data.

Azure Government infrastructure has also achieved a Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) Provisional Authorization to Operate (ATO) supporting in-scope services, including Azure Active Directory.

In addition, the Azure public cloud platform had previously received a Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) Provisional Authorization to Operate (ATO), enabling government agencies and partners to deploy moderately sensitive data to the cloud. Customers can choose either compliant environment to best meet their needs for security and isolation, with assurance that control requirements are being met by comprehensive continuous monitoring and a standardized approach to risk management in both the public and government-community clouds.

For additional information, visit the Microsoft Compliance blog and Azure Trust Center, or refer to Azure Federal Risk and Authorization Management Program (FedRAMP) Package ID# F1209051525.

The following services are Federal Risk and Authorization Management Program (FedRAMP)

authorized and approved by the Joint Authorization Board (JAB): KeyVault, ExpressRoute, WebApps, Azure Site Recovery (ASR), Microsoft Azure Backup (MAB), Notification Hubs, Service Bus, StorSimple, Automation, Azure Resource Manager (ARM), Batch, Media Services, Policy Administration Services (PAS), Scheduler, Log Analytics, and Redis Cache.

Some Infrastructure Services Branch data elements would be: Splunk Agents to provide for the Office of the Chief Information Officer (OCISO) continuous monitoring, System logs for system activity to be forwarded to OCISO Splunk. This is a hosting environment. Any data being hosted would be governed under the individual hosted system's Authorization to Operate and Privacy Impact Analysis for that given system.

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?	No
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	
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.	
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?	
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?	
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?	
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 website 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
		Phone numbers
		Medical records (PHI)
		Education Records
		Date of Birth
		Mailing Address
		Financial Account Info
		Employment Status
		Mother Maiden Name
		Driver License Number
		Other - Free text Field - CitizenshipRaceEthnicityCounty of Usual ResidenceState of Usual ResidenceMarital StatusGender, HRO/Staff Data Elements: Salary, Benefits Elections, Step/Level
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
		Patients
		Members of the public
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?	Given the dynamic nature of this platform system, it is understood that the purpose for which PII may be processed cannot be exhaustively anticipated. Component systems within this platform system can vary in their functionality and use cases and will have their own PIA describing their specific PII use purposes.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	

PIA - 6:	Describe the function of the SSN and/or Taxpayer ID.	N/A
PIA - 6A:	Cite the legal authority to use the SSN.	N/A
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Modernizing Government Technology Act of 2017
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Some component systems may and those PII data elements will be described in the component's PIA in which it applies.
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.	N/A. As described this platform system's component system will describe the SORN in its PIA where applicable.

PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains
		
		    Online
		
		Government Sources
		
		    Within the OPDIV
		
		    State/Local/Tribal

PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	OMB 0920-0017
PIA - 10B:	Identify the OMB information collection approval number expiration date.	9/30/2025
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A
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 authorize 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.	General Personnel Records, Records are maintained according with CDC's record control schedule and record control policy. In addition, the application follows GRS 20.2a.4, 20.2c, 20.6. The PII is secured using the CDC Active Directory authentication process and RBAC.

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.	As it relates to non-employees, component PIAs will address their methods in their associated PIA. Employees provide PII as a condition of employment to the CDC. Individuals can only opt-out of PII collection by not accepting employment at the CDC. Users consent to provide their information when they voluntarily register online within upstream Navigator web-application notifying users that their personal information is being collected.
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.	For applicable individuals, data notification and consent are handled by the component system collecting said data (each has its own PIA). For any individual who wishes to know if a system contains records about them that individual should submit a notification request to the applicable System Manager of the applicable SORN. The request must contain the same information required for an access request and must include verification of the requester's identity in the same manner required for an access request. For employees, a CDC-wide announcement would be made through a newsletter, supervisor briefings, or via an Office of the Director announcement.
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.	If individuals believe their PII has been inappropriately obtained, used, or disclosed, they may contact the Help Desk, or Cyber Security Program Office (CSPO) directly with any concerns regarding their PII. Individuals can contact the Help Desk via phone or email listed in the 'Help' section of Navigator system. The Help-desk phone number is 404-639-7500, and the Helpdesk email address is magichelp@cdc.gov.
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.	Administrators review system records on an ongoing basis for accuracy. These records are reviewed and user is asked to update and correct information annually.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators Developers 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.	Administrators - Perform managerial and supervisory activities for personnel. Developers - To develop cohorts for data analysis, based on age, benefit elections, etc. Contractors - Direct Contractors perform duties as assigned within the system.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	AHB Azure uses the Role-Based Access Control (RBAC) procedures to authorize system users' access to PII. These roles limit the users functionality and access to only that which is required to perform their job. Roles are granted by CDC supervisory personnel.
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.	Monitored by the Network and IT security controls which is administered by CSPO and Infrastructure Services Branch (ISB).
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.	System owners, system administrators, managers, contractors and program managers using the application undergo mandatory annual Security and Privacy Awareness Training (SAT), CDC Records Management Training and Role Base Training (RBT) to maintain their CDC network account and access to People Processing.
PIA - 22:	Describe training system users receive (above and beyond general security and privacy awareness training).	Users also are required to undergo mandatory annual CDC Records Management Training. In addition, users with significant security responsibilities are required to undergo Role Based Training (RBT).
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).	All official records are transferred or destroyed based on CDC record management policies and practices. The following records schedule applies to the system: GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records. This schedule covers records of a transitory or intermediary nature. Transitory records are routine records of short term value (generally less than 180 days). Intermediary records are those involved in creating a subsequent record. Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
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: Records are maintained according with CDC's record control schedule and record control policy. In addition, the application follows GRS 5.2 020. The PII is secured using the CDC Active Directory authentication process and RBAC. Technical: Monitored by the Network and IT security controls which is administered by CSPO and Infrastructure Services Branch (ISB). Physical: Properties and buildings are protected by guards. Access to grounds and building is controlled by ID badges and key card restrictions.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	8/24/2023
Privacy Analyst Comments:		Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	JWO Signature.docx
SOP Comments:	Approved on behalf of Beverly Walker. This PIA describes the boundary for a consolidated platform. Each component system will be described via its own PIA, with a reference to this particular platform. Many of the responses below make this indication. Finally, the list of PII and all its purposes cannot be defined due to the nature of this platform system. As stated above, each component system will describe the purpose of the associated PII in its own PIA.	SOP Review Date:	8/24/2023
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	8/25/2023
Agency Privacy Analyst Review Comments:	Comments below have been addressed by confirmation that separate PIAs will be created to address systems/subsystems where PII is collected about members of the public.	Agency Privacy Analyst Days Open:	1

Please comments below. Comments have also been provided to CDC Privacy via email.

PIA - 2	The previous PIA stated that PII is only col are collected about patients, and what are
PIA - 4	Will PII be used for the same purpose(s) fo suggests that the system will be used to re
PIA - 8B	If records about patients and/or business c
PIA - 13	How are patients and business contacts no
PIA - 14	How would patients and business contacts
PIA - 23	Does this apply to records about patients

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	
SAOP Comments:		**SAOP Review Date:**	8/25/2023
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Supporting Documentation in Response to HHS Q about PIA 2..docx	15610	.docx	8/24/2023 1:52 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 12A	BANKS, Quentin	5/31/2023	Nonresponsive. If the information submission is mandatory, please provide the specific legal requirement that requires individuals to provide information and that notes that individuals will face potential civil or criminal penalties if they do not comply with that requirement. If no legal requirement exists, then the answer to PIA-12 is voluntary.	
PIA - 18	BANKS, Quentin	5/31/2023	Please explain why each group requires access to PII individually. HHS will not accept one general answer to cover all groups.	
PIA - 19	BANKS, Quentin	5/31/2023	What is the system administrator`s process to determine who has access to the PII? What`s the reason for those individuals to have the access? Please go to question 32 of the last approved PDF PIA for guidance.	
PIA - 22	BANKS, Quentin	5/31/2023	Please include the name(s) of the training and the frequency.	
PIA - 23	BANKS, Quentin	5/31/2023	Not applicable is not acceptable for this answer. Please describe the retention and destruction process and list any Records Control Schedule (RCS) Job Numbers or General Records Schedules (GRSs) that apply to the PII maintained in the system; and/or State if the appropriate RCS Job Number or GRS for some or all of the PII maintained in the system and that the PII should be maintained until a determination is provided. **For**	

			assistance, please contact the CDC Records Management Team at records@cdc.gov . Please include your process for the retention and destruction of PII. (i.e. Records Control Schedules: DAA-0443-2012-0007-0006 or N1-443-00-002) Also, go to question 37 of the last approved PDF PIA for guidance.
PIA - 24	BANKS, Quentin	6/2/2023	Please update your GRS numbers as GRS 20 has retired.
PIA - 7	OSHODI, Jarell	7/26/2023	Executive Order 9397 involves SSNs. How is that legal authority relevant here?
PIA - 10C	OSHODI, Jarell	7/26/2023	Above a system of record notice was identified as applicable to this system. Therefore, this statement seems contradictory. How can there be a SORN without a SOR?
PIA - 10C	MOSIOS, Joshua	8/7/2023	OPM/GOVT-1, General Personnel Records is cited. Please correct or explain in a note (the yellow pad to the right of the answer prompt)