

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 - AGOL - QTR2 - 2023 - CDC6787120	PIA ID:	1674620
Name of Component:	CDC - ATSDR GRASP ArcGIS Cloud	Name of ATO Boundary:	ATSDR GRASP ArcGIS Cloud
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	322
Submission Status:	Re-Submitted	Submit Date:	4/19/2024
Next Assessment Date:	N/A	Expiration Date:	5/9/2027
Office:		OPDIV:	CDC
Security Categorization:	Low	OpDiv PIA ID:	CDC6787120
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.		9/22/2023
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.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	In previous versions, mailing addresses and phone numbers were listed collected types of PII, but were not listed in PTA-5. They have been added to PTA-5 in the user registration section of the information types collected.
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 purpose of the system is to provide data visualizations for public health data sets and to collaborate with state and local partners on shared mapping data. It supports the HHS mission of enhancing the health and well-being of all Americans by giving CDC geospatial tools that allow it to more effectively respond to public health threats and mitigate harmful environmental exposures.

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 collects, maintains and shares the following types of information:

- Geographic Identifiers (geocoded street address, state, county, zipcode);
- Facilities (type, features, etc.);
- Disease Indicators (rates, counts, demographics, etc.)
- Environmental Data (flood plans, environmental hazards, disease vector habitats, etc.)
- User Registration (name, email, organization, user name, password, phone number, mailing address)

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.	<p>ATSDR (Agency for Toxic Substances and Disease Registry) GRASP (Geospatial Research, Analysis, and Services Program) ArcGIS Cloud (AGOL) uses the Environmental Systems Research Institute (ESRI) Managed Cloud Services FedRamp certified software as a service (SaaS) offering to examine patterns and trends associated with environmental health, chronic and infectious disease, injury, and emergency preparedness and response. Datasets are either purchased from private companies, provided by federal, state, and local partners, or created by GRASP; and are typically approved for public release. The system enables users to access or upload geographic data, collaborate on shared maps, and perform specialized tasks such as geocoding.</p> <p>The system collects, maintains and shares the following types of information: Geographic Identifiers (geocoded street address, state, county, zipcode); Facilities (type, features, mailing address, phone numbers, etc.); Disease Indicators (rates, counts, demographics, etc.) Environmental Data (flood plans, environmental hazards, disease vector habitats, etc.) User Registration (name, email, organization, user id)</p> <p>The system collects and maintains geographic identifiers, facilities, disease indicators, and environmental data from state and local public health partners in order to visualize data sets and to collaborate on geospatial information.</p> <p>User registration information is collected from state and local public health partners for the purpose of account verification and authentication.</p> <p>Geographic identifiers, facilities, disease indicators, and environmental data that is cleared by CDC for public release is shared on the system's public portal. External public users are authenticated via user name and password. Internal users are authenticated by a CDC authorized system, active directory services. Active Directory has its own PIA.</p>
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 purpose of https://cdcargis.maps.arcgis.com is to provide visualizations of public health data important. The website is accessible without any login credentials and is available to the public.
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?	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 - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Mailing Address User Credentials Other - Free text Field - geocoded street address,, county, organization, phone number
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
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	501 - 2000
PIA - 4:	For what primary purpose is the PII used?	The primary purpose of the PII in the system is account verification and authentication.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Business contact information may be used to contact participating organizations.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	N/A
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.	Public Health Service Act 42 CFR § 71.21 - Report of death or illness. 5 U.S.C. Executive Orders 9397, 12862, 1302, 2951, 3301, 3372, 4118, 8347 as amended by 13478, 9830, and 12107
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 Online Government Sources 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 number is not required as the collection of information is for business PII used to assist project officers with federal funding. The respondents are employees acting within the scope of their employment for which the information is collected.

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.	<p>CDC employees give consent to business PII information collected during orientation in writing or verbally. External Users are informed PII collected will be used to support the project and is required as part of the account creation process on a project.</p> <p>Individuals who access the system may not opt-out of the collection or use of their PII because they would not be able to use the system without it being collected and used for authentication purposes.</p> <p>Public health officials who collect, aggregate, and de-identify the data supplied to the program are responsible for providing each individual with notice and choice.</p>
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.	When major changes occur to the system, affected individuals would be contacted by email to notify them of the changes and obtain their consent.
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.	When an individual has a concern that their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate, they must contact the system administrator via email at graspsharredservice@cdc.gov . Individuals should reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant. The system administrator would take appropriate action based on the information received from the individual.

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 PII in the system is user data and is provided directly by system users upon registration. Users must verify the accuracy, integrity, availability and relevancy of their PII in the system at least every 90 days or their accounts will be deactivated. No other processes are in place for periodic reviews of PII contained in the system since a user's PII can not be verified beyond what the user, as a state or local public health partner provides.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators Contractors Others
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 access PII for account verification purposes when a user has issues logging into their account. Direct contractors will serve as administrators. Administrators access PII for account verification purposes. The vendor will use PII to authenticate users to the system and troubleshoot any problems with authentication..
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Administrators (direct contractors or federal employees) and the vendor are the only users with access to all the PII in the system. Administrator level access is approved by the system's business steward after ensuring that the individual has read and signed the system's rules of behavior, completed appropriate training, and has a copy of the system's standard operating procedures. In addition, direct contractors who administer the system will be required to sign a non-disclosure agreement. Vendor procedures to determine which system users have access to PII have been vetted and approved by the Federal Risk and Authorization Management Program (FedRAMP) .
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.	Administrators (direct contractors or federal employees) and vendors need access to all PII in the system for account verification and technical support. No other users require access to PII. The system uses the least privilege model and non-administrative users are prevented from accessing PII by various controls. The controls/methods (access control lists, database partitioning, etc.) in place to only allow those with access to the minimum amount of information necessary to perform their jobs have been vetted and approved by FedRAMP.

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.	CDC users of the system must complete annual security awareness training and acknowledge the AGOL Rules of Behavior. State and local public health partners sign the AGOL Rules of behavior but do not have access to PII.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	N/A
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).	The system follows General Records Schedule (GRS) 3.2 item 30 for retention and destruction of PII. GRS 3.2-30 states that the records are temporary and should be destroyed when the 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.	<p>The administrative controls educate system users of their responsibility to protect PII and legally bind them to do so. These controls include signed rules of behavior , non-disclosure agreements, CDC privacy and security awareness training, and records management training. Records are maintained according to CDC record control policies and procedures.</p> <p>The technical controls, implemented by the system, act to either allow access to system PII data only to approved users or to make PII data unreadable outside of the system. These controls include encryption, authentication, firewalls, intrusion detection systems, and anti-malware systems.</p> <p>The physical controls, implemented by the system, restrict access to CDC buildings and areas housing computers used by this system. These controls include guards, identification badges, key cards, locked doors, cipher locks, fences, alarms and closed circuit TV.</p>

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	4/22/2024
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:	4/29/2024
		SOP Days Open:	10

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	4/30/2024
Agency Privacy Analyst Review Comments:	<p>Reviewer: Jim Laskowski</p> <p>4/30/2024 PTA-5A display "error" and PTA-5B is blank, however we know that user credentials are used to access the system specifically username and password. CDC also addressed the comment for PIA-13. This PIA is ready for SAOP review and approval.</p> <p>3/19/2024 Per CDC's email rejected the PIA.</p> <p>3/15/2024 SAOP-upon review has some concerns and email CDC Privacy for clarification.</p> <p>3/7/2024 All comment(s) have been addressed, this PIA is ready for SAOP review and approval.</p> <p>7/31/2023: While we know updates can't be made to the PTA, please address the comment for PIA-13. Is notice given to external and internal user that their PII will be collected?</p>	Agency Privacy Analyst Days Open:	1

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:	4/30/2024 PTA-5A display "error" and PTA-5B is blank, however we know that user credentials are used to access the system specifically username and password.	SAOP Review Date:	5/9/2024
		SAOP Days Open:	9

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
(2-20-2024) AGOL Privacy_Impact_Assessment_PIA_bl_jl_PA Approved.rtf	904046	.rtf	3/7/2024 1:35 PM	1
Re_ CDC PIA(s)_ CDC6787120 and CDC6736120.pdf	272514	.pdf	3/19/2024 2:41 PM	2

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	6/28/2023	<p>There are additional PII elements processed by this system. In particular, user name and password are personal identifiers. Additionally, the below information, while in isolation may not directly identify any individuals, is likely considered PII by HHS when in combination with all the various user registration information. If any of the below elements are purely isolated from any individual, please justify so to the privacy team at pia@cdc.gov.</p> <p>Geographic Identifiers (geocoded street address, state, county, zipcode); Disease Indicators (rates, counts, demographics, etc.) User Registration (name, email, organization, user name, password, phone number, mailing address)</p>	
PIA - 5	Data Feed Service, piafrmcdc	6/28/2023	Are users contacted? If so, the aforementioned user registration PII serves a secondary purpose as a method of communication.	
PIA - 10C	Data Feed Service, piafrmcdc	6/28/2023	A justification is required if an OMB number is not provided.	
PIA - 1	LASKOWSKI, JAMES	7/31/2023	The reviewer notes that PTA-5A, PTA-5B and PTA-12A did not sync.	
PIA - 13	BLAND, CRYSTAL	7/31/2023	IS a notice provided informing the individuals (internal and external) that there PII will be collected? If so please include in your response.	

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:	5/9/2024 8:03 PM	History Log:	View History Log
---------------	------------------	--------------	----------------------------------