

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 - AIPIMS - QTR4 - 2023 - CDC7092087	PIA ID:	2804350
Name of Component:	CDC - Arctic Investigations Program Information Management System	Name of ATO Boundary:	Arctic Investigations Program Information Management System
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	489
Submission Status:	Re-Submitted	Submit Date:	3/18/2025
Next Assessment Date:	N/A	Expiration Date:	3/23/2028
Office:		OPDIV:	CDC
Security Categorization:	Moderate	OpDiv PIA ID:	CDC7092087
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.		
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.	None
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.	<p>The purpose of the Arctic Investigation Program Information Management System (AIPIMS) is for the prevention of infectious diseases in people of the Arctic and sub-Arctic with a special emphasis on diseases of high incidence and concern among the Alaska Native and other northern indigenous peoples. Arctic Investigation Program (AIP) conducts infectious disease surveillance, evaluate prevention services, and conduct applied research in collaboration with partners.</p> <p>AIPIMS is a web-based application that provides an integrated system for tracking of laboratory specimens and associated epidemiologic study data which are associated with specimens received at AIP. The application is used to collect, process, store, and report medical research data.</p>

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.	<p>The system stores data contains the associated demographics and sample informatics for the large specimen collection maintained at AIP for the Alaska Area Specimen Bank. Participant information is collected directly from participants who are advised of the purpose of the information as described in each studies institutional review board (IRB) approved protocol.</p> <p>AIPIMS is an internal system and users are authenticated through Personal Identity Verification (PIV) card and Active Directory. Passwords are not stored anywhere within the system, but user ids, which are CDC network user IDs, are stored in database permanently.</p> <p>Participant Personal Identifiable Information (PII) is collected, processed and stored. The AIP system collects PII information including Date of Birth, Name, Medical Records Number, Mailing Address, E-Mail Address, Phone Number, Mother's Maiden Name, and Medical Notes.</p>
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>The AIPIMS is used to conduct infectious disease surveillance, evaluate prevention services, and conduct applied research in collaboration with our partners. It collects, stores, processes, and reports medical research data. The system collects PII information including Date of Birth, Name, Medical Records Number, Mailing Address, E-Mail Address, Phone Number, Mother's Maiden Name, and Medical Notes for medical research purposes.</p> <p>The AIPIMS system provides support for research studies on the control and prevention of infectious disease. It provides an IT platform for laboratory and epidemiology work done by the Arctic Investigations Program (AIP).</p> <p>AIPIMS is an internal system and users are authenticated through PIV card and Active Directory. Passwords are not stored anywhere within the system, but user ids, which are CDC network user IDs, are stored in database permanently.</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)?	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.	Only CDC internal users access the web application through CDC Active Directory (AD). It's used to support for research studies on the control and prevention of infectious disease. It provides an IT platform for laboratory and epidemiology work done by the Arctic Investigations Program (AIP). AIPIMS is an internal system and users are authenticated through PIV card and Active Directory. Passwords are not stored anywhere within the system, but user ids, which are CDC network user IDs, are stored in database permanently.
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?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Does Not 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) Date of Birth Mailing Address Medical Records Number User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	PII provides the information for identifying and tracking laboratory specimens associated with epidemiological studies conducted at Arctic Investigations Program and specimens in the Alaska Area Specimen Bank.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Also, study participant data are collected, processed, and stored for research purposes.
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, Section 301, "Research and Investigation," (42 U.S.C. 241); and Sections 304, 306 and 308(d) which discuss authority to maintain data and provide assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)).
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.	Medical Notes, medical records, and patient data are all 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.	09-20-0136 : Epidemiologic Studies and Surveillance of Disease Problems. HHS/CDC
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Non-Government Sources Members of the Public
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 Collection # 0920-1254
PIA - 10B:	Identify the OMB information collection approval number expiration date.	3/31/2026
PIA - 10C:	Explain why an OMB information collection approval number is not required.	Not Applicable
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.	Individuals may choose not to sign a consent form and not participate in the study. Participants always have the option to withdraw from studies at any time. They additionally have the option to participate in an Arctic Investigations Study, but can opt out of their specimen being stored within the Alaska Area Specimen Bank, negating the need to store PII. And in addition, they are provided a phone number, that they can call to have their information removed at any point in the future. They are provided with the information per IRB approved methods.
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.	Should any major changes to the system occur, the SORN would be modified and republished to reflect those changes. Under this scenario, and if necessary, the Arctic Investigations Program (AIP) would prepare to re-consent with individuals by contacting them directly with the help of their respective Alaska Native Health Corporation. In Person contact is made with individuals.

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.	Individuals may contact program manager or the Alaska Area Specimen Bank director. All participants are provided with this contact information when being consented into an Arctic Investigations Program study. They can 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 Alaska Area Specimen Bank director and the program manager then jointly correct the problem. The department manager can be contacted by phone or email and is in the office five days per week. System technical steward does all the work on this system. He can be contacted by phone or email. He is in the office Tuesday through Friday and teleworks Mondays. Both of them are also available by Skype.
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.	Every six months, twenty randomly chosen lab slips containing PII are compared against the PII in the AIP system. Any necessary corrections are reviewed to ensure the AIP system is not the cause of the inaccuracies. Staff verify PII information against lab slips, Lab Manager has the final review, and System owner perform ad-hoc comparisons.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers
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.	Users- To Enter PII data and conduct research Administrators- Maintain operating system and database management system Developers- Maintenance of the application along with any associated system changes
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The Role-based access is used in the AIPIMS system. After a user is approved to access the system, the user will be created and assigned to a user group with predefined roles and access privilege. The group roles and access privilege are determined by AIPIMS system business steward, management, and subject matter experts. In AIPIMS system there are 5 different user groups, Administrator, Data Management, Lab Technicians, Epi Staff, and Statisticians, each with different roles and data access privilege.

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 AIPIMS system employs the concept of least privilege by ensuring that each job role is performed by a different individual. Ensure all users conduct duties with only the privilege necessary to perform their respective, and separate job functions. The AIPIMS system has 5 different group users: Administrator, Data Management, Lab Technicians, Epi Staff, and Statisticians. Administrators are assigned and monitored by Program Management, Business Steward and Contracting Officer's Representative. Administrators are required to complete CDC's Security Awareness Training and Role Base Access Control training. Other users, based on mission requirements and approval by Business Steward may gain read/write or read only access to the system. The AIPIMS system administrators create unique profiles for each user and assign users to user groups.
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.	All AIPIMS users receive annual Security and Privacy Awareness Training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	All AIPIMS users with access to PII receive annual Role-Based Training.
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).	Application owners follow Federal and HHS policies and guidelines regarding retention and destruction of PII data. Records are retained and disposed of in accordance with the CDC Records Control Schedule. Record copy of study reports are maintained in agency from two to three years in accordance with retention schedules. Source documents for computer are disposed of when no longer needed by program officials. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records are retained for 20 years; for longer periods if further study is needed. System adheres to the CDC Records and Retention schedule GRS 5.7, DAA-GRS-2016-0016-0002, and DAA-GRS-2016-0016-0003.

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 include Federal, HHS, and CDC specific Privacy, Risk Assessment, and Incident Management Policies, annual system privacy impact assessments; and mandatory annual security & privacy awareness training.

Technical Controls include the Data Entry module can only be accessed by CDC registered users that have CDC network access using a smartcard. User access to AIPIMS system is further limited by application level role based access controls. PII data is encrypted both in transit and at rest. In addition, server audit, accountability measures, and continuous monitoring of system resources to identify vulnerabilities are enforced to ensure the system's adherence to organizationally defined minimum security requirements.

Physical controls include gated campuses with 24-hour guards to enforce access restriction; key card access to campus buildings. Access to the data entry center is only available to smartcard holders inside CDC facilities where there is also physical CDC security.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	3/18/2025
Privacy Analyst Comments:		Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	
SOP Comments:	Approved on behalf of Beverly Walker	SOP Review Date:	3/19/2025
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	3/20/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 3/20/2025 No comments. This PIA is ready for SAOP review and approval.	Agency Privacy Analyst Days Open:	1

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:		SAOP Review Date:	3/24/2025
		SAOP Days Open:	4

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	2/24/2025	Please add Date of Birth. PTA 5 states that CDC user IDs are stored in the database. Is the user ID stored within the AIPIMS system or within active directory? Please update as applicable.	
PIA - 2	Data Feed Service, piafrmcdc	2/24/2025	You indicated in the last PIA that PII from employees is collected, please update as applicable. Are you still	

collecting PII from employees? If you are not, when and why did you stop collecting data from employees and who approved it.

PIA 9 Lists members of the public but PIA 2 list just patients (are these direct patients of the program or is the program receiving the data from another party? please update as applicable avoiding contradictory information.

PIA - 10C	Data Feed Service, piafrmcdc 2/24/2025	Please explain why an OMB number is not required if the data is of patients/members of the public. Is this because of research data?
PIA - 11	Data Feed Service, piafrmcdc 2/24/2025	<p>who are the partners as mentioned below? Is the data shared with other non-CDC healthcare providers or non-governmental sources? Are the Alaska Native Health Corporation, Area Specimen Bank director CDC workers? if data is shared, please update as applicable.</p> <p>The description states that AIPIMS is used to conduct infectious disease surveillance, evaluate prevention services, and conduct applied research in collaboration with our partners. It collects, stores, processes, and reports medical research data.</p>
PIA - 14	Data Feed Service, piafrmcdc 2/24/2025	How are they contacted? is it via email and/or phone?
PIA - 16	Data Feed Service, piafrmcdc 2/24/2025	Who is doing the comparison, please add to the narrative.
PIA - 17	Data Feed Service, piafrmcdc 2/24/2025	BSI page 8 mentions CDC-Contractors, please update as applicable.
PIA - 18	Data Feed Service, piafrmcdc 2/24/2025	Please explain why contractors' need access since they are mentioned in the BSI on page 8.
PIA - 19	Data Feed Service, piafrmcdc 2/24/2025	Add the explanation for contractors as indicated in PIA 17 and 18
PIA - 20	Data Feed Service, piafrmcdc 2/24/2025	Administrators are assigned via contract and monitored by Program Management, Business Steward and Contracting Officer's Representative but there is no mention of contractors in PIA 17, 18, and 19. Please review and update as

			applicable.
PIA - 21	Data Feed Service, piafrmcdc	2/24/2025	The role-based training mentioned in PIA 20 should be moved to PIA 21
PIA - 22	Data Feed Service, piafrmcdc	2/24/2025	The role-based training mentioned in PIA 20 should be moved to PIA 21
PIA - 1	Data Feed Service, piafrmcdc	3/10/2025	Please see comment above and update as applicable. PTA 5 states Participant Personal Identifiable Information (PII) is collected, processed and stored. The AIP system collects PII information including Date of Birth, Name, Medical Records Number, Mailing Address, E-Mail Address, Phone Number, Mother's Maiden Name, and Medical Notes.
PIA - 9	Data Feed Service, piafrmcdc	3/10/2025	Please see comment in PIA 2, if PII is collected from members of the public please also indicate in PIA 2.
PIA - 10C	Data Feed Service, piafrmcdc	3/10/2025	Please answer the question. opt out is not a valid response. If information is collected from members of the public, then an OMB number is required. See comment above.
PIA - 18	Data Feed Service, piafrmcdc	3/10/2025	After clarification that contractors only have access to deidentified data, please remove contractors.
PIA - 8A	Data Feed Service, piafrmcdc	3/18/2025	Are any direct identifiers used to retrieve the records? What's listed does not indicate a direct identifier. Are there any identifying numbers, names, etc. that uniquely identify an individual?
PIA - 8B	Data Feed Service, piafrmcdc	3/18/2025	If records are not retrieved by a direct identifier, please delete this response.
PIA - 1	BLAND, CRYSTAL	3/20/2025	On the next iteration of the PTA: PTA-5A respond "Yes, but user credentials are maintained by another system: Active Directory."

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:	3/24/2025 4:01 PM	History Log:	View History Log
---------------	-------------------	--------------	----------------------------------