

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 - PRFWKS - QTR2 - 2023 - CDC6735746	PIA ID:	1661185
Name of Component:	CDC - Poxvirus and Rabies Freezerworks Inventory	Name of ATO Boundary:	Poxvirus and Rabies Freezerworks Inventory
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	375
Submission Status:	Submitted	Submit Date:	3/1/2024
Next Assessment Date:	N/A	Expiration Date:	1/1/2100
Office:		OPDIV:	CDC
Security Categorization:	Low	OpDiv PIA ID:	CDC6735746
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.		4/5/2024
5:	Is the system or electronic information collection, agency or contractor operated?		Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	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.	The purpose of the Poxvirus and Rabies Freezerworks Inventory (PRFWKS) is to keep inventory records for all long term storage samples in the poxvirus and rabies lab. The system allows users to input information on where samples are stored, when they are added, and removed, along with all pertinent information about each sample. The program is also used to print labels for samples and to create reports for laboratory regulation requirements.

<p>PTA - 5:</p>	<p>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>	<p>The software provides the ability to create and print bar code labels for samples. Users are able to input information on where samples are stored in refrigerators and freezers, when they are added, when they are removed, along with all pertinent information such as the sample characteristics (sera, virus, clinical samples, etc.) and the usage of samples by members of the lab (stored by user ID) about each sample. PRFWKS is also used to print labels for samples and to create reports for laboratory regulation requirements.</p> <p>PRFWKS is an internal system and users are authenticated to the CDC internal network through PIV card and Active Directory (AD); AD is a separate system with its own PIA.</p> <p>The users of the PRFWKS system are also assigned a user id and passwords that are stored in the system until the user is removed from the system. The user password is created by the user.</p>
<p>PTA - 5A:</p>	<p>Are user credentials used to access the system?</p>	<p>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</p>
<p>PTA - 5B:</p>	<p>Please identify the type of user credentials used to access the system.</p>	<p>Non-HHS User Credentials</p> <p>Username</p> <p>Password</p>
<p>PTA - 6:</p>	<p>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>	<p>PRFWKS allows users to input shelf/row location, the type of sample being stored and date of the placement. Users can be assigned to groups to restrict views to certain data entry screens, freezers, data views, and other functionality in the software. The software provides the ability to create and print bar code labels for samples. Users are able to input information on where samples are stored in refrigerators and freezers, when they are added, when they are removed, along with all pertinent information such as the sample characteristics (sera, virus, clinical samples, etc.) and the usage of samples by members of the lab (stored by user ID) about each sample. PRFWKS is also used to print labels for samples and to create reports for laboratory regulation requirements.</p> <p>PRFWKS is an internal system and users are authenticated to the CDC internal network through PIV card and Active Directory (AD); AD is a separate system with its own PIA.</p> <p>The users of the PRFWKS system are also assigned a user id and passwords that are stored in the system until the user is removed from the system. The user password is created by the user.</p>
<p>PTA - 7:</p>	<p>Does the system collect, maintain, use or share PII?</p>	<p>Yes</p>
<p>PTA - 7A:</p>	<p>Does this include Sensitive PII as defined by HHS?</p>	<p>Yes</p>

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 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.	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.	51 - 200
PIA - 4:	For what primary purpose is the PII used?	The userid/password are used for login (access) to the system.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	None
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); sections 304, 306 and 308(d) which discuss authority to grant 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.	
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.	Government Sources Within the OPDIV
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.	Data is collected from within agencies.
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 option to opt-out is not available. If users opt out, they will not have access to the PRFWKS system to perform their job duties.

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, the administrator will notify the individuals who have accounts in the system via group email, phone calls or face to face meetings with the laboratory group.
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 an individual believes their information has been inappropriately obtained, used, disclosed, or the PII is inaccurate, they can contact the POC listed in this document.
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.	User accounts are audited annually by the program to determine if there are still requirements for each to have an account of the system. If a user is no longer required to have access, they are removed from the system by system administrator.
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.	Access to userID required to create user accounts.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The Role-Based Access (RBAC) is used in the PRFWKS system. Only administrator may access business PII information. After an 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 roles and access privileges are determined by PRFWKS system business steward, management, and subject matter experts.
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.	PRFWKS utilizes the Least Privilege Model for granting application level access to system data. The data is accessible by the authorized personnel only. The Least privilege model is used to provide Read only access according to predefined roles. User access is limited to job function and information only essential to the user function.
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 PRFWKS users receive Security Awareness and Privacy Training on an annual basis.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	All PRFWKS users receive 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).

Final reports and substantive reporting materials are maintained permanently. Routine reports are maintained for five years. Other input/output records are disposed of when no longer needed. 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. PRFWKS system adheres to the CDC Records and Retention schedule GRS 5.2, item 020, N1-442-09-01, item 3 (), and N1-442-09-01, item 4.

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:
Only authorized CDC staff, contractors, and guest researchers have access to the data, all of whom receive the appropriate Privacy and role-based trainings prior to access. No data will be allowed to be downloaded to or to reside on a portable device (e.g. laptops, thumb drives, storage media). PII is secured in the system via FISMA compliant Management, Operational, and Technical controls documented in the systems security authorization package.

This include Federal, HHS, and CDC specific Privacy, Risk Assessment, and Incident Management Policies, as well as annual system privacy impact assessment reviews.

Technical Controls include application level role based access controls; servers audit and accountability requirements; encryption of PII at rest and in transit; and adherence to organizationally defined minimum security controls.

Physical Controls:
Security is provided by housing PRFWKS servers in a secured facility protected by guards and a cardkey system. Access to the computer room is controlled by a PIV card and security code (numeric keypad) system. Access to the data entry area inside of the lab buildings, the laboratories themselves, and offices near the laboratories is controlled by a PIV card.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	3/4/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: March 4, 2024	Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	
SOP Comments:	Approved on behalf of Beverly Walker	SOP Review Date:	3/18/2024
		SOP Days Open:	17

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	3/28/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 3/28/2024 All comments have been address, this PIA is ready for SAOP review and approval. PTA-5: We know that the user Id is store in the system is password also stored? PTA-5A states that the user credentials are used to access the system, but they're maintain by another system. CDC response for PTA-5/PTA-6 does not provide the name of the system and whether that system is covered in a separate PIA. Please explain.	Agency Privacy Analyst Days Open:	10

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Update PTA-7A in next iteration as CDC noted it was mistakenly selected Yes.	SAOP Review Date:	4/30/2024
		SAOP Days Open:	33

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
(3-25-2024) Re_ CDC PIAs.pdf	223836	.pdf	3/25/2024 3:08 PM	0
Re_ CDC - PRFWKS - QTR2 - 2023 - CDC6735746.pdf	270208	.pdf	4/29/2024 4:47 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	9/30/2024	This System has been migrated within the OCIO MSP Hosting Services authorization boundary. All future updates should be made via the new Sub- Component application.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	Is OpDiv Privacy Analyst Return ? :	0
Is Agency Privacy Analyst Approve ?:	1	Is SOP Return ?:	0
Is SAOP Approved?:	1	Is Agency Privacy Analyst Return ?:	0
Total Approved:	4	Is SAOP Return ?:	0
Total Approval Required:	4	Total Return:	0

Miscellaneous Fields

Last Updated:	9/30/2024 8:01 PM	History Log:	View History Log
---------------	-------------------	--------------	----------------------------------