Privacy Impact Assessment (PIA): CDC - SG - QTR2 - 2023 - CDC6742861

Created Date: 7/19/2023 11:55 AM Last Updated: 9/30/2024 8:01 PM

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 - SG - QTR2 - 2023 - CDC6742861	**PIA ID:**	1679923
Name of Component:	CDC - SampleGuard	**Name of ATO Boundary:**	SampleGuard
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	364
Submission Status:	Re-Submitted	**Submit Date:**	10/27/2023
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Low	**OpDiv PIA ID:**	CDC6742861
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.	8/5/2020
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.	SampleGaurd is designed to monitor CDC laboratory cryo-freezers, and raise alerts (for CDC laboratory personnel to evaluate) via email and the application console if the freezers appear to be performing outside of satisfactory range.

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 data collected by the system consist of operational readings of cryo-freezer performance within CDC laboratories, and performance thresholds against which the measures are compared. If the operational readings of freezer performance fall outside the acceptable thresholds, alerts are generated by the system and sent via email to selected laboratory personnel via their CDC email accounts. Logs and freezer performance readings are owned by CDC. The system is strictly internal, with few internal users. Authentication is Standard internal user only controlled by Active Directory. Other than performance metrics and thresholds, the additional data includes inventory descriptions of the freezers and the CDC email of the laboratory personnel selected to receive the alerts. SampleGuard monitors laboratory freezers in CDC laboratories. If the freezers operate out-of-range, SampleGuard sends to the email addresses of selected laboratory employees using their cdc.gov email addresses. There is no other PII, and no other use of the CDC email addresses.
PTA - 5A:	Are user credentials used to access the system?	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
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.	SampleGaurd is designed to monitor CDC laboratory cryo-freezers, and raise alerts (for CDC laboratory personnel to evaluate) via email and the application console if the freezers appear to be performing outside of satisfactory range. The data collected by the system consist of operational readings of cryo-freezer performance within CDC laboratories, and performance thresholds against which the measures are compared. If the operational readings of freezer performance fall outside the acceptable thresholds, alerts are generated by the system and sent via email to selected laboratory personnel via their CDC email accounts. Logs and freezer performance readings are internal. Other than performance metrics and thresholds, the additional data includes inventory descriptions of the freezers and the email of the laboratory personnel selected to receive the alerts. The data is used to create emailed alerts and to profile the performance of CDC laboratory cryo-freezers and is not exported or shared with any other systems. SampleGuard monitors laboratory freezers in CDC laboratories. If the freezers operate out-of-range, SampleGuard sends to the email addresses of selected laboratory employees using their cdc.gov email addresses. There is no other PII, and no other use of the CDC email addresses.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No

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.	SampleGuard website monitors laboratory freezers in CDC laboratories. If the freezers operate out-of-range, SampleGuard sends to the email addresses of selected laboratory employees using their cdc.gov email addresses. only CDC authorized personel have access. There is no other PII, and no other use of the CDC email addresses.
PTA - 10:	Does the website have a posted privacy notice?	No
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	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
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 PII is used to create email alerts for the performance of CDC laboratory cryo-freezers.
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, 42 U.S. Code § 300u
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.	Information is not sourced from the public.
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 Sampleguard 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 program will provide a written notice to the individuals who have accounts in the system. This notification will occur via email, phone or face to face meetings.
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.	The SampleGuard Rules of Behavior state that system administrators will, at a minimum, annually review the PII for integrity, availability, accuracy and relevancy. They also have the right to review the PII collected at any time, if they suspect integrity, availability, accuracy, or relevancy has been compromised.
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 user ID is required to configure email alerts.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Only application Administrators would have access to the production data and users emails. No users will have access to any PII. SampleGuard management assigns specific system administrators the authority to access, write, update, and maintain.
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.	Access for internal CDC system administrators is determined on a case-by-case basis by the to SampleGuard SampleGuard 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 SampleGuard users receive Security Awareness Training on a annual/yearly basis.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Reading the SamlpeGuard system's Rules of Behavior and signing the accompanying acknowledgement.

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).	SampleGuard Data is retained and disposed of in accordance with the CDC Records Control Schedule: Per GRS 5.2, Records are stored for 2 years to allow CDC access to the information when requested. After two years, data is purged from the database.
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, and contractors, 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. 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 SampleGuard 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:**	11/6/2023
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Re-Approved Date: November 6, 2023	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	See Comments Comments Addressed upon Review #2. Approved by Beverly E. Walker, CDC SOP	**SOP Review Date:**	3/25/2024
		SOP Days Open:	150

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	3/25/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte All comments have been addressed. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	0

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	4/29/2024
		SAOP Days Open:	35

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 9	Data Feed Service, piafrmcdc	10/13/2023	Your response seems incomplete given that you state also @ Q2 that PII is also collected re Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors). What is the	

			source of this PII?
PIA - 13	Data Feed Service, piafrmcdc	10/13/2023	Response as written is acceptable WRT employee PII -- what about the PII of the vendors, etc as identified in Q2?
PIA - 2	Data Feed Service, piafrmcdc	10/13/2023	Inconsistency ...In your PTA, you only mention and explain the use of employee email addresses; however, you now include another category of individuals from whom PII (presumably only email addresses) are maintained. Either your PIA is correct (in which case you will need to alter your PTA to account for this additional category in your responses), or the PTA is correct (in which case you will need to edit several responses in this PIA)
PIA - 4	Data Feed Service, piafrmcdc	10/13/2023	What are vendor email addresses used for?
PIA - 15	Data Feed Service, piafrmcdc	10/13/2023	May need editing dependent upon whether you're also collecting vendor and others' emails as previously stated as your current response only addresses employees. Also, even if only employees PII is involved, that does not in and of itself constitute a reason for the lack of a process. At a minimum, insofar as employees, your response might describe the incident/breach reporting process. 3rd parties, if applicable, would also need a process.
PIA - 16	Data Feed Service, piafrmcdc	10/13/2023	Suggest a rewrite as follows: The SampleGuard Rules of Behavior state that system administrators will, at a minimum, annually review the PII for integrity, availability, accuracy and relevancy. They also have the right to review the PII collected at any time, if they suspect integrity, availability, accuracy, or relevancy has been compromised.
PIA - 22	Data Feed Service, piafrmcdc	10/13/2023	Since you mention a RoB that is specific to the system in a prior question, then your response here can be Reading the SamlpeGuard system's Rules of Behavior and signing the accompanying acknowledgement.
PIA - 23	Data Feed Service, piafrmcdc	10/13/2023	I believe Schedule 23 has been

			superseded. Suggest that you check with the CDC Records Manager, Mary Wilson, or your local Records Liaison for guidance/confirmation.
PIA - 23	VILLAFUERTE, NESTOR	3/25/2024	Please define acronym "GRS" on the first instance.
PIA - 1	Data Feed Service, piafrmcdc	9/30/2024	This System has been migrated within the OCIO ISB Infrastructure 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 SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

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