Privacy Impact Assessment (PIA): CDC - EeQMS - QTR1 - 2024 - CDC7446148

Created Date: 1/26/2024 3:04 PM Last Updated: 3/1/2024 7:01 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 - EeQMS - QTR1 - 2024 - CDC7446148	**PIA ID:**	1759989
Name of Component:	CDC - Enterprise Electronic Quality Management System	**Name of ATO Boundary:**	Enterprise Electronic Quality Management System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	36
Submission Status:	Re-Submitted	**Submit Date:**	2/1/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC7446148
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)?	No
4:	ATO Date or Planned ATO Date.	3/1/2024
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

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.	Name change from OLSS Enterprise Electronic Quality Management System (OLSS EeQMS) to Enterprise Electronic Quality Management System (EeQMS)
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 this system is to develop a commercial cloud-based off-the-shelf (COTS) Enterprise electronic quality management system (EeQMS) that can interoperate and scale to support multiple CDC laboratories. The EeQMS vendor will work with the CDC EeQMS implementation team to configure the COTS cloud-based enterprise EeQMS system to support all identified laboratories, support required modules, applications and functions, extract artifacts (i.e., documents, Non Conforming Events (NCE), Corrective Active Preventive Action (CAPA) events from current eQMS tools, modules and applications, and import into the system, interface with other CDC systems (e.g., HHS Learning Portal, National Center Immunization Respiratory Diseases (NCIRD) Inventory Management System, eLIMS) where necessary, and maintain a high level of IT security in a high performance environment. Ongoing EeQMS vendor support will include maintaining EeQMS compliance with regulatory requirements, maintaining system up-time and performance, and mitigating software defects and security vulnerabilities
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 following types of information will be maintained: 1) Documents/Standard Operating Procedure (SOP) for each CDC laboratory 2) Training materials related to SOP 3) Nonconforming events 4) Corrective and Preventive Actions 5) Calibration and Maintenance records related to laboratory equipment 6) Proficiency Testing CDC Users are authenticated via Salesforce inherent authentication plus the ability to login through the CDCC Secure Access Management Service (SAMS). The system does not use Personal Identity Verification (PIV) card and a waiver was approved due to the requirements to enter the CDC high and maximum containment laboratories. CDC can be authenticated externally via Secure Access Management System (SAMS) by using a Username and Password.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	

PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	The following types of information will be maintained: 1) Name, work email, and work phone number 2) Documents/SOPs related to scientific protocols will be collected and stored through direct input by verified users. Documents will be shared to other verified users within the system. 3) Experiment inactivation checklists and procedures will be collected and stored through direct input by verified users. Checklists will be shared to other verified users within the system. 4) Basic information about each lab – number of people, tests/results, types of hazards, accreditation, and location. This information will only be shared with an identified set of users. 5) Users will be authenticated within the system using both Secure Access Management Service (SAMS) with a unique user ID and password. SAMS User IDs and passwords of permanent users will be stored within the system. Passwords are only stored on the system for log-in and personal notification purposes; administrators do not have access to passwords. All information will be collected through in-application forms using proper data validation and data encryption techniques to ensure data is entered correctly and is only visible to the correct group of users. Individuals submit information to the CDC application directly within the system using forms and document upload tools. Their names, email addresses and phone numbers are collected in order to contact them later. Users are asked to verify their submission before the information is passed onto to SMEs and board members for review. Users receive notification each time the status of their request changes, or when a new user receives access to the submitted information. All changes or updates to the information are archived in an audit log. Once the information is confirmed, that package is stored and all relevant users are notified.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	No
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	
PTA - 10:	Does the website have a posted privacy notice?	
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	

PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government 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 Phone numbers Certificates Education Records Devices Identifiers User Credentials Other - Free text Field - Training record
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.	501 - 2000

PIA - 4:	For what primary purpose is the PII used?	The email addresses are used to create a person's profile to allow access to the system. Email addresses and phone number may be used to contact system users as needed. Lab incidents, accidents, and quality compliance issues data that may include individual names or information that can indirectly identify individuals . Individual's education records, certificates, and training records are maintained within the system to provide objective evidence of qualification to perform tasks associated with an individual's job description/role. This objective evidence is required to be readily available during regulatory, statutory, and other quality audits.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Maintaining quality management system records including documents, training, nonconforming events, corrective and preventive actions, and proficiency testing.
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.	The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030; Identity Theft Enforcement and Restitution Act, P.L. 110-326, 122 Stat. 3560 (2008).
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 In-person Email 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.	No information is collected from general 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.	PII (name, email and phone number, UserID) is only used to verify individual users before granting them access to the system/their account and for accessing specific records created, revised, or signed off. User identification/verification is a standard/best practice when developing systems that host sensitive data. In addition, PII will not be shared or distributed. There is currently no policy in place regarding an individual opting out of the collection or use of their PII. Users are prompted to log into the system and must complete system training prior to using the system If an individual chooses to not use the system and opt out of the collection or use of their PII, they will have to communicate their objection to their manager and Chief Information Officer leadership. The result of an individual opting out would be their inability to access the tool.
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.	PII only pertains to name and email when logging into the system. Therefore, notifying and obtaining consent from users during their first log-on attempt after a critical update is feasible and effective in communicating with users and has been implemented
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.	The OLSS Support Team will respond to any concerns raised by a CDC employee. Concerns and requests are submitted via the lab quality email (labquality@cdc.gov) and triaged to members of the OLSS Support Team. The OLSS Support Team will reach out to appropriate personnel to determine the nature of the concern. A member of the OLSS Support Team will communicate issues and findings from this analysis to 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.	There are currently no processes in place for the periodic review of PII. The PII in the EeQMS system is limited to static information pertaining to a user's profile for accessing the system. The user's information is limited to name, user ID, work email, and work phone number. Once in the system, a user's profile is kept for the life of the system. This is necessary to meet regulatory and quality standard requirements related to a user's qualifications and training records

PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	Third-Party Contractor (Contractors other than HHS 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.	Users have access to their own PII only to access the system and revise contact information. Administrators will perform functions related to staff onboarding and system configuration. Third party vendor as Developers will assist with the entry of data and will migrate data and system configurations into the production environment. Third party vendor as Contractors will assist with the entry of data and will migrate data and system configurations into the production environment
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	User permissions and roles identify who will have access based on the least privileged principle. Only branch superusers that have the rights and permissions to add new staff members to the system will be able to access PII within the EeQMS system. The number of branch superusers will be limited to one primary and one secondary per branch. The branch super users will be responsible for performing some administrative functions, such as adding/removing system users and configuration updates/changes within their specific branch. The super user administrative rights and permissions will be limited to staff and functions within their assigned branch.
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.	All users must be approved by the Administrators based on their role, duties and responsibilities prior to gaining access to the data. Role Based Access Control (RBAC) is utilized. The roles are predefined, users are assigned those roles as appropriate. Only branch super users will be granted the rights and permissions required for accessing PII. The rights and permissions granted to each superuser will be limited to staff and functions within their specific branch. Administrators and reviewers are required to review specific relevant documents.
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.	Annual Security and Privacy Awareness training is required for all CDC employees and contractors.

PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	All system users will receive training prior to being granted access to the system. The training will include standard operating procedures (SOPs), notes and emails about the system. This training will be a one-time training administered by a system super user prior to users being granted access to the system. Additional training will be administered only upon system upgrades and/or revisions to the applicable SOPs.
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).	Records are maintained in accordance with GRS 2.7 040: Occupational Safety and Health Administration (OSHA) regulated substance monitoring and exposure records. Temporary. Destroy no sooner than 30 years after monitoring is conducted, but longer retention is authorized if needed for business use. When data is deleted, it is still temporarily available (15 days) to customers on-line from their recycling bin. In order to permanently remove deleted items, the user will empty the recycle bin. Upon emptying the recycle bin, customer data that is deleted could still live on Salesforce backups. Salesforce retains system backups for 90 days, therefore customer deleted data would be completely purged after 90 days when backups are overwritten. Salesforce is a separate system covered by a separate PIA.
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 a system security plan, contingency plan, regular back up of files and storage of backups off site, role-based security awareness training, separate user and privileged accounts or administrators, policies and procedures in place for retention and destruction of PII, and a corporate incident response team and incident response plans. Technical: Identification and authentication using unique User IDs, passwords, and smart cards, use of firewalls and intrusion detection/prevention systems, and virus scanning software on all computers. Role based access controls are in placing using Active Directory permissions. Physical: Controls are managed by security guards, ID badges and key card restrictions.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	2/5/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: February 5, 2024	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	2/8/2024
		SOP Days Open:	7

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/9/2024
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Signature.docx
SAOP Comments:	Approved on behalf of Bridget Guenther	**SAOP Review Date:**	3/1/2024
		SAOP Days Open:	21

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 7	Data Feed Service, piafrmcdc	1/26/2024	Apologies for missing this in the previous review. Please provide a legal authority for this system.	
PIA - 1	BLAND, CRYSTAL	2/9/2024	Update for the next iteration of the PTA: PTA-5A: Please select "Yes, but user credentials are maintained by another system..."	

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:	3/1/2024 7:01 PM	**History Log:**	View History Log