Privacy Impact Assessment (PIA): - QTR2 - 2024 - FDA2128117

Created Date: 4/15/2024 12:04 PM Last Updated: 1/23/2026 12:59 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:	- QTR2 - 2024 - FDA2128117	**PIA ID:**	1805590
Name of Component:		**Name of ATO Boundary:**	
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	18
Submission Status:	Submitted	**Submit Date:**	4/12/2024
Next Assessment Date:	N/A	**Expiration Date:**	4/29/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA2128117
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
2:	Is this a FISMA-Reportable system?	
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	11/1/2024
5:	Is the system or electronic information collection, agency or contractor operated?	

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
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 Center for Biologics Evaluation and Research (CBER) IdeaScale system is a cloud-based innovation management platform that enables CBER to modernize the way in which CBER conducts its internal and external crowdsourcing campaigns (collecting information and opinions from a group of people via the internet). The key functional elements of the system include a fully integrated online platform that promotes increased CBER employee/external stakeholder engagement and the sharing of ideas agency wide. CBER uses IdeaScale to regularly monitor employees' views regarding products and services, communications, relationships, and attitudes regarding the overall work environment. CBER will also use the system to gain insight from industry stakeholders (external) regarding CBER's regulated product scientific areas of interest. Users of the system include Food and Drug Administration (FDA) employees (CBER permanent and Direct Contractors) and external stakeholders (members of the public). Separate access portals are used for internal and external campaigns. Non-Agency users will not have access to the internal CBER IdeaScale employee portal. CBER IdeaScale does not interface with other FDA systems. System access requires Single-Sign On (SSO) authentication for all FDA internal users. External users of the system require username and password to access the external facing system. All responses to CBER-sponsored crowdsourcing campaigns are saved on IdeaScale servers.
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.	CBER IdeaScale collects the following personally identifiable information (PII) from CBER employees (permanent and Direct Contractors): (a) first and last name; (b) work email address; and (c) work phone number. Employee PII is obtained from the FDA Active Directory (AD, the subject of a separate assessment) where FDA maintains it in AD for the duration of an individual's employment with FDA. Retention periods for employee submissions that have been rejected or are no longer subject to consideration for a crowdsourcing campaign or retention periods as otherwise described in the Terms of Use agreement will vary depending on the subject matter of the campaign. Upon the completion of a campaign the system owner reviews submitted information to evaluate any possible need for continued retention of such documents. If the system owner determines the files are no longer needed, they will be subject to deletion according to applicable records schedules. User data/profiles will be collected and maintained in CBER IdeaScale until business use ceases under General Records Schedule (GRS) 3.2, item 030 – System Access Record.

The following non-PII is collected from CBER permanent employees and Direct Contractors: (a) FDA Center/Office name.
The system also collects the following PII from and about external stakeholders (members of the public): (a) first and last name; and (b) work email address. The system also generates and maintains PII consisting of usernames and passwords for external users. External stakeholders also submit non-PII consisting of occupation, and requests and suggestions related to CBER business operations and products. Depending on the context and association with other submitted or available data, non-PII may become PII.

CBER IdeaScale is used by CBER crowdsourcing campaign participants (CBER permanent employees, Direct Contractors and external stakeholders) who are asked to provide feedback regarding the overall CBER work environment and CBER products and services. All system users will enter text using IdeaScale's open text field. Information, suggestions, requests, and other submissions are provided directly by permanent employees and Direct Contractors through the IdeaScale employee portal. For instances where submissions may be sought from external stakeholders, these users may provide their suggestions, requests, and other submissions through the IdeaScale external non-employee portal. System users who would like to remain anonymous can do so by selecting one of three available privacy and anonymity features (anonymous idea submission; private submission; or hidden identity). Users will need to navigate to the CBER IdeaScale frequently asked questions (FAQ) landing page to confirm privacy/anonymity settings.

FDA reviews all submissions on a regular basis. FDA system administrators (Admins) have the ability to modify or remove content.

User credentials are collected and maintained in the system. For Agency users, employee names, email addresses, office affiliations, and phone numbers are obtained from the FDA AD. External users must provide their name and email address when accessing IdeaScale via the non-employee portal. This information is necessary to create username and passwords for external users and control system access. All data provided by external users will be maintained in IdeaScale servers for registration/login purposes.

Other data maintained and shared from the system include the opinions, requests, and suggestions of CBER permanent employees, Direct Contractors, external stakeholders, and Admin

		approvals.
PTA - 5A:	Are user credentials used to access the system?	Yes
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.	CBER IdeaScale will be used by crowdsourcing campaign participants (CBER permanent employees, Direct Contractors, and external stakeholders) to provide feedback regarding the overall CBER Work environment and CBER products and services. CBER uses the information collected to increase employee engagement and service/product innovation. Information collected from non-Agency engagement will allow external stakeholders to express their ideas and be active participants in identifying scientific needs/opportunities for FDA. PII collected from CBER employees (permanent and Direct Contractors) will include employee name, work email address, and work phone number. PII collected from non-Agency participants will be limited to the individual's name, email address, username and password. The first and last names of individuals responding to a campaign will be available for view by other users of the system. If an individual submitter does not want their name to be shared with other users, users have the option to submit campaign responses anonymously. Email addresses will not be shared with or viewable by non-Admin users of the system. Individuals who wish to email other users of the system may do so while logged in to the system. Email addresses will be shared with and viewable by system Admins only. IdeaScale system Admins will use PII (names and email addresses) to retrieve campaign responses for follow up communications with campaign submitters.
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)?	Yes
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The purpose of the website is to provide users access to IdeaScale to submit requests, opinions, and suggestions for CBER management review and approval. Users access IdeaScale using SSO authentication (internal users) or username/password (external users) via publicly viewable URLs.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	Yes
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes

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.	
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?	Yes
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.	The purpose of the IdeaScale mobile application is to provide external users access to the system using their mobile devices. External users access the mobile application via public URL. https://fda-cber.ideascalegov.com/
PTA - 16:	Does the mobile application/ have a privacy notice?	Yes
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	Yes
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	Yes
PTA - 18:	Does the mobile application use measurement and customization technology?	Yes
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	Persistent Cookies – does not collect PII
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	No
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?	Yes
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 Employment Status User Credentials Other - Free text Field - FDA Center/Office name

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.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	The FDA uses the PII for communication purposes only. Following campaign submissions, FDA will use this information to follow up with campaign participants.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The FDA makes no secondary use of the PII collected
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Establishment and use of this system is authorized by 5 U.S.C. 301, 305; 21 U.S.C. 301; 44 U.S.C. 3101; E.O. 13571. The security and privacy measures employed in the application are required by the Federal Information Security Modernization Act (FISMA) and statues underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	The PII data elements that are used to retrieve record and members of the public).
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.	SORN 09-90-1901, HHS Correspondence, Comment, Customer Service, and Contact List Records
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Non-Government Sources Members of the Public

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.	This is not an official FDA form or query where information is being collected; an OMB collection approval number is not required.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Private Sector
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	PII (names and email address) will be disclosed to system Admins when follow up is necessary to clarify an idea, question, or comment submitted. Admins are Direct Contractors.
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)).	https://fda-cber.ideascalegov.com/a/register-Terms of Agreement.
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.	Users of the system are advised that name is the only identifying information that will be displayed when submitting content in the IdeaScale system. However, users who wish to remain anonymous when submitting content may choose to do so by navigating to the IdeaScale FAQ landing page and selecting one of three available privacy and anonymity features (anonymous idea submission; private submission; or hidden identify). To the extent required under law, regulation or policy, the designated System Owner maintains an accounting (log) of disclosures. The Privacy Office is available to provide guidance to the System Owner.
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.	There is no option to object to or opt-out of the information collection if a user wants to contribute to the campaign. An interested party/user is required to create a login using PII in order to contribute to a crowdsourcing campaign. However, users who wish to remain anonymous when submitting content may choose to do so by navigating to the IdeaScale FAQ landing page and selecting one of three available privacy and anonymity features (anonymous idea submission; private submission; or hidden identify).
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.	No such changes are planned or anticipated. If changes are made, notifications would be communicated by IdeaScale with appropriate FDA direction as needed.

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.	Site moderators review all idea submissions before general posting on the platform to ensure they do not violate the Terms of Use. Any individuals who suspect their PII maintained by or on behalf of the FDA has been inappropriately obtained, used or disclosed have several avenues available to resolve the situation. These individuals may contact the office or division where they have determined that their information is held. They may contact the FDA Privacy Office via email address provided on FDA.gov. Employees with such concerns can work with their supervisors, the FDA Privacy Office, Employee Resource and Information Center (ERIC), FDA's Systems Management Center, and other channels. Contact information for these offices and resources is available across FDA's internet and intranet pages. FDA personnel are required to rapidly report any suspected incidents or breaches to the FDA Cybersecurity Infrastructure Operations Coordinating Center (CIOCC). Contractors are required to safeguard all information and to report potential data breaches to the FDA.
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.	Individuals voluntarily provide their PII and are responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information themselves. PII relevancy is supported through the design of the system and user processes to require and collect only that PII which is necessary to administer the system and enable its intended use. Access is granted and restricted at the individual level (role-based access). Integrity and availability are protected by privacy and security controls selected and implemented in the course of providing the system with an authority to operate (ATO). Controls are selected based on NIST guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Administrators: require access to PII about users to facilitate follow-up communications associated with employee/external user submissions. Contractors: may be granted "Administrator" status when needed to build and support the campaigns. Admins have access to PII.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Only those Agency Admins running the campaigns will be allowed access to the users PII.
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.	Technical methods such as system-specific access set access to PII to only access the minimum amount of
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.	FDA users will not receive additional training other than the general security and privacy training provided by FDA. Agency and contractor site/system moderators/administrators are required to complete the mandatory FDA security awareness training given annually which includes required privacy awareness training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	No additional system-specific training is received by users, however users can access user guides and manuals and privacy guidance on the FDA intranet and from Privacy staff. User guidance and resources are also available via links accessible on the webpages associated with the system.
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).	FDA and supporting will maintain records in CBER IdeaScale based on the subject matter of the campaign. Retention periods may differ. Upon completion of each campaign the information will be reviewed by the System Owner to evaluate any possible need for continued retention of such documents. If the System Owner determines the files are no longer needed and need not be maintained under record keeping requirements, they will be subject to deletion. User data/profiles will be maintained in CBER IdeaScale until business use ceases under the National Archives Records Administration (NARA) citation GRS 3.2, item 030 – System Access Records: Information Technology/Electronic Records- Temporary: Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.
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 safeguards include role-based access restriction, user training, securely configuring the system, and reviewing audit logs; implementation of need-to-know and minimum-necessary principles when awarding access. Technical controls include access controls, use of firewalls and other Federal Risk and Authorization Management Program (FedRAMP) controls including applicable National Institute of Standards and Technology (NIST) and Federal Information Security Modernization Act (FISMA) controls. Physical controls include system servers housed in locked FDA facility and use of security guards.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	4/15/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	4/15/2024
		SOP Days Open:	3

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	4/23/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 4/23/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	8

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	4/29/2024
		SAOP Days Open:	6

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
CBER IdeaScale_SOP Approved.pdf	188390	.pdf	4/16/2024 7:25 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

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:	1/23/2026 12:59 PM	**History Log:**	View History Log