PTA / PIA: FDA - External Crowdsourcing - QTR3 - 2025 - FDA4972349

Created Date: 9/23/2025 12:37 PM Last Updated: 11/20/2025 3:32 PM

General Information

PTA / PIA Name:	FDA - External Crowdsourcing - QTR3 - 2025 - FDA4972349	**PTA / PIA ID:**	3850821
Component Name:	FDA - CDER External Crowdsourcing	**ATO Boundary Name:**	CDER External Crowdsourcing
Overall Status:	Complete	**# of Days - Open:**	58
Submitter:		**Submit Date:**	9/23/2025
Next Assessment Date:	11/19/2028	**Expiration Date:**	11/19/2028
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	6/23/2023
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Mark Ascione
PTA 01A:	POC Title and Organization	Operations Research Analyst FDA/CDER/Office of Strategic Programs (OSP)/Office of Program and Strategic Analysis (OPSA)/ Program Evaluation and Implementation Staff (PEIS)
PTA 01B:	POC Email Address	ascione@fda.hhs.gov
PTA 01C:	POC Phone Number	301-796-7652

PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The subject of this assessment is the Food and Drug Administration (FDA) Center for Drug Evaluation and Research (CDER) External Crowdsourcing platform. The CDER External Crowdsourcing system is a structured, public-facing platform that facilitates idea submissions, community engagement and internal project planning. CDER External Crowdsourcing uses IdeaScale, a third-party owned Software as a Service (SaaS) Federal Risk and Authorization Management Program (FedRAMP) authorized cloud provider to facilitate use of the external crowdsourcing platform. FDA controls access and use of the CDER External Crowdsourcing platform. CDER External Crowdsourcing brings together members of the general public (e.g., patients, caretakers, researchers, and industry professionals) and internal users of the system (FDA permanent employees and Direct Contractors) to collect diverse input on regulatory and drug development. FDA can make customizations to the platform and control a lot of what the public views and engages with when they use our external crowdsourcing platform. Senior FDA leaders use the CDER External Crowdsourcing system to submit questions related to specific areas of interest (also known as "challenges") and invite internal and external users of the system to provide feedback that may be used to inform ongoing and future FDA initiatives. Users participate by submitting ideas, commenting on other participant ideas, or voting on ideas that others have presented. Participants registered within Ideascale can submit answers to specific questions (or “ideas”) that can be viewed on the “challenge” page and do so anonymously. Participants may also elect to identify themselves when posting, however an individual must self-select the opt-out feature made available by the system. The FDA also provides transparency for whether an idea is being incorporated. For example, a senior leader who wants to know how a specific rare disease affects the day-to-day life of patients can pose that question as a challenge to a target audience and use the feedback received to shape subsequent discussions and drug development or other initiatives related to the disease. Internal users represent FDA when moderating external discussions and answering questions from other users. Most challenges target patients, advocates, and caregivers but other stakeholders will engage at times as well. Members of the public can access external crowdsourcing without an account, however external users who wish to post/comment must create a free account to do so.

PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	CDER External Crowdsourcing collects and maintains personally identifiable information (PII). PII is collected from internal and external users of the system. Data collected and maintained in the system includes user specific information, user responses to FDA challenges/topics (e.g., identify research topics for FDA, tell us about your experience, etc.), and/or user voting outcomes. PII collected and maintained about internal users of the system (FDA employees and Direct Contractors) may include information typically associated with account information, business email address and first and last name. PII associated with external users of the system includes personal or business email address, first and last name and user credentials (applicable for those with accounts and includes password only). PII may also include unsolicited medical information (e.g., experience with illness, treatment, etc.) as provided by the user on a voluntary basis. PII in the system is stored on a temporary basis and disposed of in accordance with National Archives and Records Administration (NARA) record control schedules.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Password Email Address
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	Information collected and maintained by CDER External Crowdsourcing is shared with IdeaScale to authorize system user access and allow for the participation in external crowdsourcing. Email address and first and last name are collected about internal users of the system. PII about external users of the system includes email address, first and last name, user credentials (those with accounts) and possibly medical information (e.g., detailing experience with illness, treatment, records, etc.) as provided voluntarily by external users.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	https://shareyourvoice.ideascalegov.com
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes

PTA 09:	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 enable FDA personnel and members of the public (target audience based on topic may include patients, caretakers, researchers, etc.) to provide feedback to the questions submitted by FDA senior leaders. Participants registered within Ideascale can also submit answers to specific questions which are called “ideas." The website allows participants to submit ideas, comment on other participant ideas, or vote on ideas that others have presented. FDA employees and Direct Contractors access the platform through Single Sign On (SSO) authentication methods. Members of the public (who wish to view and post responses) access the platform by entering their user credentials which is email address and password.
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?	No
PTA 12:	Does the website use web measurement and customization technology?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies- Collects PII
PTA 12C:	What PII is collected by the web measurement and customization technology?	Name and email address.
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Biographical Information Name User Credentials Contact Information Email Address (Personal) Email Address (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Volunteered Medical Information (experiences with various diseases and treatments). User credentials for external users include email and password only.

PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Patients Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	PII is used to facilitate the participation of FDA personnel and members of the public in FDA sponsored crowdsourcing events.
PIA 26:	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.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The implementation of this system is authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	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 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	The requirements of the Paperwork Reduction Act (PRA) do not apply to social media and patient experiences.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	Email address and name is for internal users. Email and user credentials (password) is used for external users. Information is collected by the underlying platform to create user accounts and authenticate users.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	There are no agreements for information sharing or disclosure with the public. CDER External Crowdsourcing hosts an online public forum.
PIA 32D:	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.	User activity is accounted for using system logs which capture account creation and access.
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Individuals may opt-out of the collection or use of their PII by not participating in crowdsourcing activities. Employees and external account holders who wish to access the system must provide their PII. Users can post anonymously.
PIA 35:	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). If they cannot be notified or have their consent obtained, explain why.	If CDER changes the collection, use, or sharing of PII data in External Crowdsourcing, CDER will notify affected individuals by the most efficient and effective means available and appropriate to the specific change(s). This notice may include a phone call, a mail notification, a notice on a web site, or email notice to the individuals.
PIA 36:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have several avenues available to resolve the situation. External users of the system may contact the office or division where they have determined that their information is held. Individuals may then make further requests for their information to be corrected or amended. FDA considers these requests and, if appropriate, makes the requested changes. Internal users (employees and Direct Contractors) with such concerns may contact their supervisors, the Privacy Office, the Employee Resource Information Center (ERIC), the Cybersecurity Infrastructure Operations Coordination Center (CIOCC), and other channels listed on FDA's internet and intranet pages. FDA personnel must immediately report all known or suspected breaches.

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	PII is provided voluntarily by the individual. Each individual (user) is responsible for providing accurate information and may ensure accuracy by reviewing their submission content before submitting it. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. The relevancy of the PII is ensured by the design of this system which limits the PII collected to that which is necessary. PII integrity and availability are protected by security controls selected and implemented in the course of providing the system with an authorization to operate (ATO). Controls are selected based on National Institute of Standards and Technology (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. CDER performs annual reviews to evaluate user access. One of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified in the course of system use are addressed when discovered.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: require access to their own PII to access the system. Administrators: require access to PII to create and manage user accounts. Some administrators are Direct Contractors. Contractors: Some of the users are Direct Contractors who serve in administrator positions; some third-party contractors require access while performing specific, contracted service or functions. Developers: may require access when troubleshooting an issue that is negatively impacting the user experience.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Only those FDA employees and Direct Contractors who serve in a system administrator role may access PII not their own. Access is granted on a need-to-know basis. Non-administrator users and external users will only have access to their own PII. The Agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Role based access controls (RBAC) including Administrator controlled technical settings are employed to ensure that users have only the necessary access to perform their job duties. Management establishes roles for individual personnel, with role-based restrictions permitting access only to information that is required for each individual to perform his/her job.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All internal system users at FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Information Management and Technology (OIMT) verifies that training has been successfully completed.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Additional training is not provided.
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	CDER maintains system records under Agency records schedule FDA 9991a2 – Information Technology (IT) Development Project Records. The NARA approved citation is GRS 3.1, Item 011, System Development Records. Disposition: Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

PIA 45:	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 user training, system documentation that advises on proper use, implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical safeguards include role-based access settings, firewalls, passwords and others. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology (NIST) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	9/23/2025
Privacy Analyst Review Comments:	Archer error associated with question General 03: “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” The FDA instance of Archer is automatically entering the answer “No” which is incorrect. It should be "yes" and the ATO date is 6/23/23. At this time, we are unable to update Archer to reflect the correct answer.	**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	9/23/2025
SOP Review Comments:	The FDA’s Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	11/17/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 11/17/2025 Emailed regarding the expired ATO date but didn't receive a response, however, the PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	55

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	11/20/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	3

SAOP Signature

Date	User	Type	Name	Original Value	New Value
11/20/2025 11:18 AM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	VILLAFUERTE, NESTOR	9/25/2025	Q3 states that the system does not have an active ATO, however, the given date has passed.	
PTA 12A	BLAND, CRYSTAL	9/25/2025	disregard	
PTA 01	BLAND, CRYSTAL	11/17/2025	11/17/2025 Emailed FDA on 9/25/2025 regarding the expired ATO and requested for a planned ATO. We have yet to receive a response.	9-25-2025 EMAIL_FDA - External Crowdsourcing - QTR3 - 2025 - FDA4972349.pdf