Privacy Impact Assessment (PIA): FDA - pFDA - QTR4 - 2024 - FDA4323695

Created Date: 10/15/2024 12:23 PM Last Updated: 10/23/2024 2:43 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:	FDA - pFDA - QTR4 - 2024 - FDA4323695	**PIA ID:**	2321475
Name of Component:	FDA - OC PrecisionFDA	**Name of ATO Boundary:**	OC PrecisionFDA
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	12
Submission Status:	Submitted	**Submit Date:**	10/15/2024
Next Assessment Date:	N/A	**Expiration Date:**	10/23/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4323695
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.	8/2/2023
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.	FDA has made no changes to PrecisionFDA since the last Privacy Threshold Analysis/Privacy Impact Assessment was approved.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Contractor

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.	System Purpose, Functionality and Users PrecisionFDA (pFDA), an online, cloud-based portal that allows scientists from industry, academia, government, and other partners to come together to foster and develop the science behind a method of reading DNA known as next-generation sequencing (or NGS). NGS allows scientists to compile a vast amount of data on a person's exact order or sequence of DNA. Recognizing that each person's DNA is slightly different, scientists can look for meaningful differences in DNA that can be used to suggest a person's risk of disease, possible response to treatment and assess their current state of health. Ultimately, the differences that are learned can be used to design a treatment tailored to a specific individual thus the precision portion of the name. PrecisionFDA was designed in response to the Precision Medicine Initiative of 2015, announced by President Barack Obama in his 2015 State of the Union Address to collect genetic and health data from one million subjects. In October 2016, the project was renamed 'All of Us'. The pFDA system is a specially designed portal that leverages the commercially available DNAnexus Platform (Platform). This portal allows scientists to upload any files and run any Linux software, but the typical use cases involve users uploading the digital output of their DNA sequence machines understanding the variations of the DNA against reference genomes, comparing bioinformatics pipelines and sharing benchmarking-related genomic data. The users of the pFDA system see only the functionality of the underlying Platform that is revealed through the pFDA portal. The underlying Platform is a secured cloud-based system accessible via the Internet. Users interact with the pFDA via secure web access. This interaction may include uploading data, managing, running and running software, and collaborating with fellow users.
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 types of information collected into the system are : User's name and email address The types of data that are maintained in and/or shared from the system is/are: The user’s name and email address is shared with the support team and the administrators of the system for timely operation of the system. The amount of time the PII is stored in the system is: Indefinitely per the requirements of the system.
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.	HHS User Credentials HHS/OpDiv PIV Card HHS Email Address HHS Username Non-HHS User Credentials Username Password Email Address
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 information is collected and/or maintained in order to manage the ownership and, user's accountability and operation of the system. We collect this information as a basis for operating user accounts on the Platform and when necessary, providing support to individual users. Accounts associated with user's name and email address are used for the administration of the users, inviting users to Challenge activities on the system and identifying parties on discussions. The categories are on users who (1) administer the scientific functionality of the system and (2) users who participate in the scientific activities of the system.
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 the genomic community with a secure, cloud-based platform where participants can access and share datasets, analysis pipelines, and bioinformatic tools, in order to benchmark their approaches and advance regulatory site. The following categories of individuals have access to the website: Food and Drug Administration (FDA), Department of Health and Human Services (HHS), Centers for Disease Control and Prevention (CDC), and Department of Agriculture employees. Public users include academic and medical researchers, clinicians, pharmaceutical companies, and non-US regulatory agencies. Users access the website via public URL and requesting an account. FDA accounts are protected by the FDA's SSO/PIV card. Non-FDA users have a unique username, password and multi-factor authentication.
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.	Persistent Cookies - Does Not 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?	Yes

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Grantees Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000

PIA - 4:	For what primary purpose is the PII used?	PII is used for operating the system. The collected PII allows basic usage of user accounts on the Platform and when necessary, providing support to individual users. Accounts associated with user's name and email address are used for the administration of the users, inviting users to Challenge activities on the system and identifying parties on discussions.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	FDA makes no secondary use of the PII.
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.	The legal authorities that govern information use and disclosures specific to the system and program are: See Section 6.3 of the FISMA SSP.
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 Online Other Non-Government Sources Members of the Public Other
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.	An OMB information collection number is not required because the type of information collected does not require PRA clearance.
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.	There is no option to opt-out of the collection. Not providing the requested PII will result in the user not being given access to the system.
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 process in place to notify: Consent is collected as a condition of applying for access to the system. There are no expected changes that would necessitate obtaining additional consent. However, if any changes are made, users can be notified via email.
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 processes in place to resolve an individual's concerns when they PII has been inappropriately obtained, used or disclosed include: The processes in place to resolve an individual's concerns when they believe that PII has been inappropriately obtained, used or disclosed include: The user can request a "subject access request," pursuant to requesting a "write to be forgotten" request. This would be handled by the underlying FedRAMP processes that are inherited by the FISMA authorization.
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 process in place for periodic reviews of PII to ensure the data integrity is: PII is audited on a weekly basis as part of the underlying FedRAMP controls supporting the FISMA "Moderate" system. The process in place for periodic reviews of PII to ensure data availability is: The PII review is part of the larger weekly security reviews of all users of the underlying FedRAMP system. The process in place for periodic reviews of PII to ensure data relevancy is: The PII review is part of the larger weekly security reviews of all users of the underlying FedRAMP system. Accuracy of PII is ensured: The accuracy of the FDA users is high due to the integration with the FDA SSO system. The accuracy of the non-FDA data is self-reported making the accuracy unqualified.
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.	The reason the following groups need access to PII is: To approve users, operate the system, and provide support Users access PII about themselves and other users to have access to the usernames of participants working within their FDA-sponsored challenges. Administrators require access to PII about users to to approve users, operate the system, and provide support. Contractors help perform the administration of the scientific content, load the data for the Challenges, and provide 1st and higher level support to the PrecisionFDA users. Contractors also monitor the user requests and user activity to enforce the controls required by the FISMA authorization, the underlying leverage of the FedRAMP systems, and to comply with the applicable laws and regulations pertinent to the PrecisionFDA system.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The administrative procedures in place to determine which system users may access PII are to approve users, operate the system, and provide support.
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.	The following technical methods are in place to allow those with access to PII to only access the minimum amount of information necessary to perform the job: Inherited controls from the supporting FedRAMP “Moderate” systems.
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 users for PrecisionFDA are required to complete the following training and awareness programs to make them aware of protecting PII: The standard Agency training for FDA and Direct Contractor personnel (using FDA courses). There is also inheritance of privacy training from the FedRAMP “Moderate” CSO.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	System users also receive the following additional training: Security, Privacy, software development processes, data retention training, and user guides.
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).	The records in pFDA are maintained under General Records Schedule (GRS) 3.1. The National Archives Records Administration (NARA) citations used are N1-88-04-05 for significant research project records, N1-88-04-05 for non-significant research project records, and N1-88-04-05 for research project working paper records. The disposition of records is temporary. The records are destroyed 5 years after the project is terminated, 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.	FDA secures PII in the system using the following administrative controls: In accordance with FISMA "Moderate" ATO for the system. FDA secures PII in the system using the following technical controls: In the FISMA ATO. Administrative and technical controls include: CA-3(04) – security and privacy representatives are part of the configuration change control reviews in the underlying FedRAMP "Moderate" CSO. PM-18 – The Privacy Policies are inherited from the underlying FedRAMP "Moderate" CSO PM-19 – The Privacy Program leaders are inherited from the underlying FedRAMP "Moderate" CSO PM-20: The privacy policies are are inherited from the underlying FedRAMP "Moderate" CSO as well as stated on the landing page and footer of every page of the application. PM-20(01) - The privacy policies are are inherited from the underlying FedRAMP "Moderate" CSO as well as stated on the landing page and footer of every page of the application. PT-05(02) a. Develops FDA privacy reports and disseminates to: 1. FDA oversight bodies to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and 2. FDA officials and other personnel with responsibility for monitoring privacy program compliance; and b. Reviews and updates privacy reports at least annually.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	10/15/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP 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.	**SOP Review Date:**	10/15/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	10/16/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 10/16/2024 All comments address, this PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	10/23/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
OC PrecisionFDA SOP approved.pdf	165274	.pdf	10/16/2024 9:53 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 9	Data Feed Service, piafrmfda	10/11/2024	PII is provided when an account is approved and provisioned on the system. For non-FDA users, this information is self-reported. For FDA users, the PII is aligned with the FDA Single Sign On (SSO)	
PIA - 21	VILLAFUERTE, NESTOR	10/16/2024	Please define acronym "CSO"	
PIA - 21	BLAND, CRYSTAL	10/16/2024	CSO stands for FedRAMP Moderate Cloud Service Offering (CSO)	

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:	10/23/2024 2:43 PM	**History Log:**	View History Log