Privacy Impact Assessment (PIA): FDA - DataFit - QTR3 - 2024 - FDA3614280

Created Date: 8/19/2024 12:03 PM Last Updated: 8/28/2024 2:31 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 - DataFit - QTR3 - 2024 - FDA3614280	**PIA ID:**	2131505
Name of Component:	FDA - CDER DataFit	**Name of ATO Boundary:**	CDRH Scientific and Research General Support Systems
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	12
Submission Status:	Submitted	**Submit Date:**	8/16/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA3614280
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?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	1/10/2023
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.	The system holds anonymous clinical trial data supplied by sponsors of New Drug Applications (NDAs) to assist reviewers in their analyses. This was previously recorded as personally identifiable information (PII), however, since the clinical data is completely anonymous and unable to be linked to an individual, this PIA is being updated to reflect that.
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.	Food and Drug Administration (FDA) Center for Drug Evaluation and Research (CDER) Office of Computational Science (OCS) changes how data from regulatory submissions to the FDA is acquired, stored, and analyzed to produce quantitative-based decisions by the agency. CDER utilizes a set of review tools to provide drug submission reviewers with services to aid their review. These tools are referred to as CDER Study Data Review Tools (SDRT), in which DataFit is a component. This PIA addresses DataFit. FDA maintains separate PIAs for the other mentioned components. DataFit is used to validate submissions to assess conformance of clinical and non-clinical trial data to industry and FDA business rules. The application establishes an understanding of the submitted data and shows the impact to standard safety analysis and review tools based on data quality issues in the submission. DataFit users are FDA reviewers and Direct Contractors who provide reports and support.
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.	DataFit collects the following Personally Identifiable Information (PII): First and last names, and work email addresses for FDA employees and Direct Contractors. The PII in this system is not shared with any other system or organization. DataFit uses sponsor-supplied clinical trial data. Clinical trial participants have information collected about them, including subject numbers, demographic information, adverse events, and other health information. DataFit validates the data to determine if the data fits industry standards and business rules. This information is not stored in DataFit. DataFit is directed to a data facility that exists at the FDA called Data Central and validates the data from there. None of this information is personally identifiable.
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
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 about clinical trial subjects is collected and/or maintained in order to enable the review process of submissions to approve / reject new medicine approvals. PII from the system/component/collection about users of the system is not shared with other systems or outside parties.
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?	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 Mailing Address User Credentials
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 primary purpose of the PII used in the DataFit is to identify points of contact consisting of FDA employees and Direct Contractors for account management and to communicate operational information.
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.
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 the core of the FDA / CDER's purpose to approve and maintain safety of medicines. PDUFA is a legal authorization in this area. 5 U.S.C. 301.
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 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.	N/A. The PRA does not apply to CDER DataFit because no data is collected from the public.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	

PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	FDA personnel are required to provide their PII as a requirement of working at the FDA and performing their job functions. There is no opt option to opt out. If an individual chooses not to provide their PII, they will not be able to work at the FDA in this role.
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.	If the Agency makes any major changes in the collection or use of PII in CDER DataFit, FDA will notify the affected individuals in the most efficient and effective manner available and appropriate, which may include a formal process involving written or electronic notice, or informal processes such as 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.	Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any of the tools comprising SDRT have multiple options available to resolve the issue. These individuals may contact FDA via email, phone and standard mail avenues (all of the relevant contact information is listed on fda.gov). They may also contact FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). Additionally, individuals may raise concerns through supervisory channels and through the FDA’s Employee Resource and Information Center (ERIC).
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 submit their PII consisting of professional contact information. The individual submitting the PII is responsible for providing accurate information. Integrity and availability are protected by 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. CDER performs annual reviews to evaluate user access. Data discrepancies identified in the course of system use are addressed when discovered.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators Developers 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: For troubleshooting production level system problems. Some of the Administrators are Direct Contractors. Developers: For system development and testing purposes. Some of the Developers are Direct Contractors. Contractors: Direct Contractors whose roles are assigned as administrators and/or developers.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Administrators and developers are required to have elevated privileges in order to access the full system and its data. FDA utilizes an Access Control system that requires pre-access approval from system owners and supervisors. Application-specific procedures include requesting access from business, system, and data owners and approval through supervisors.
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.	DataFit uses individual role-based accounts to ensure minimum necessary access. DataFit maintains an access control procedure which outlines the steps to request role-based access. The roles include, at a minimum, “administrator” and “user.” Other roles include variations of the user role. The system, business, and/or data owner will authorize access to the system with supervisory approval. The administrator of the system will set the appropriate degree of access. All users are authenticated by FDA enterprise wide SSO, Active Directory, or username/password combination. Once a user is authenticated by FDA, credentials are passed to the tool, and the tool will provide access based on the role.
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 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 - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	System/system component/information collection users also receive the following additional training: Users are provided with user guides hands on instructional guidance by a team of CoreDF analysts who coach end users on how to utilize the system outputs. Privacy guidance is available on the FDA intranet and from Privacy staff.

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 DataFit are maintained under the following National Archives and Records Administration (NARA) citations: General Records Schedule (GRS) 3.2 items 30 and 31. The records disposition is temporary under disposition authority DAA-GRS2013-0006- 0004 and the records are deleted or destroyed 6 years after they are no longer needed or when business use ceases.
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 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 use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	8/16/2024
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:**	8/19/2024
		SOP Days Open:	3

Agency Privacy Analyst Review

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

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	8/28/2024
		SAOP Days Open:	5

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

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:	8/28/2024 2:31 PM	**History Log:**	View History Log