





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 - CDER DASH - QTR3 - 2024 - FDA2375432	PIA ID:	2020659
Name of Component:	FDA - CDER Data Analysis Search Host	Name of ATO Boundary:	CDER Office of Regulatory Operations
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	24
Submission Status:	Submitted	Submit Date:	7/9/2024
Next Assessment Date:	08/02/2027	Expiration Date:	8/2/2027
Office:		OPDIV:	FDA
Security Categorization:		OpDiv PIA ID:	FDA2375432
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)?		Yes
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.	<p>The system is comprised of several individual applications and tools. The following tools are in Center for Drug Evaluation and Research (CDER) Study Data Review Tools (SDRT): Janus, Evaluation of Drug Induced Serious Hepatotoxicity (eDish), Portes, MediaWiki, DataFit, iPortal, Investigational New Drug (IND) Smart Template, Institutional Review Board (IRB), and Data Analysis Search Host (DASH).</p> <p>Since the last privacy assessment was conducted, the DASH component of SDRT now intends to collect personally identifiable information (PII).</p>
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 SDRT and include: Empirica Study, JReview, MedDRA Adverse Event Diagnostics (MAED), JANUS, eDISH, Portes, Media Wiki, Datafit, iPortal, IND Smart Template, IRB, and DASH.
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.	Empirica Study, JReview, MAED, Janus, iPortal, Portes, DataFit, and DASH collect the following Personally Identifiable Information (PII): First and last names, and work email addresses for FDA employees and Direct Contractors. Additionally, Empirica Study collects access credentials consisting of username and password for FDA employees and Direct Contractors. DASH additionally collects first and last names for advisory committee participants, which can be found in publicly available documents on FDA.gov. The PII in these systems is not shared with any other system or organization.
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.	<p>The systems of the Study Data Review Tools encompass comprehensive tools that help reviewers understand, analyze, and use data so they spend more time thinking about the results of the data analyses rather than setting up those analyses. The tools provide data management, data fitness assessment, exploratory safety, and other analyses.</p> <p>Portes manages, validates, and versions CDER submission/study data. Empirica Study provides a mechanism for repeatable drug safety analyses of clinical trial data. It can assess data pulled from CDER Electronic Document Room (EDR) from specific clinical trials and pool data across clinical trials and across Non-Disclosure Agreements (NDAs) and Biologic License Applications (BLAs). JReview allows users to analyze safety and efficacy data obtained from CDER EDR. It enables users to visualize data graphically. MAED Tool performs a series of exploratory adverse event (AE) analyses. CDER Wiki is a MediaWiki system that acts as a collaboration tool for reviewers, serving as a knowledge base and centralized repository to consolidate, modify and share regulatory and nonregulatory information to build historical documentation. Janus Non-Clinical is a data repository for validated Clinical Data Interchange Standards Consortium (CDISC) Standard for Exchange of Nonclinical Data (SEND) compliant study data submitted by sponsors in support of INDs, BLAs and NDAs. It provides Non-Clinical Reviewers a vehicle to review non-clinical studies. Janus Non-Clinical allows reviewers to interact directly with study data to create tables and figures that can be included in review documents. JANUS Clinical is a data repository application that supports the extraction, validation, transformation, loading, and management of standard clinical trials data in a secure database and provide reviewer access to that data via extract databases.</p> <p>SDRT Tools are directly aligned with the FDA mission by ensuring the safety, efficacy, and security of human and biological products. This includes alignment with Agency Priority Goals 678: Foster and apply innovative solutions to health, public health, and human services challenges; 670: Improve healthcare quality and patient safety; and 472: Improve health care through meaningful use of health information technology.</p>
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 User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Members of the public
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 collection of the PII in DASH is for granting access to DASH for the system users. The PII stored in DASH is used for access credentials, to facilitate the login process for FDA reviewers.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The secondary use of the PII in DASH is for contacting the system reviewers (FDA employees and direct contractors). DASH additionally collects first and last names for advisory committee participants, which can be found in publicly available documents on FDA.gov. This information is used to help facilitate the searching of participants that voted in past advisory committee meetings that may be good candidates for future/upcoming meetings.
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.	5 U.S.C. 301; 21 U.S.C. 301 (Federal Food, Drug and Cosmetic Act)
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Email 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.	DASH utilizes FDA employees and contractors to identify Advisory Committee voting member information from member rosters already collected and reported via publicly available sources.
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.	DASH users who voluntarily elect to be granted access may not opt-out of providing PII because it is required to administer access through single sign-on procedures.
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 FDA changes its practices with regard to the collection or handling of PII related to the DASH system, the agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.
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 may submit questions or comments about the DASH PII to a dedicated email address. Questions or comments about PII submitted to this address will be routed to the DASH system owner who will handle any PII issues and consult or advise privacy and security officials as needed. If there is a need to remove or correct any PII in DASH, the system owner will instruct members of the DASH data entry team to modify the data in the DASH database as required. If the DASH data entry team has any technical difficulties modifying the data as instructed, they may contact the DASH System Administrators for assistance.
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.	SH data analysts follow data entry procedures outlined in the DASH standard operating procedure (SOP) to ensure data integrity. Analysts also conduct a quarterly Quality Assurance Quality Control (QAQC) of all data within DASH to ensure accuracy. The availability of the DASH system is limited to employees within CDER that have been granted access.
PIA - 17:	Identify who will have access to the PII in the system.	Users 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.	<p>Users: Users will perform queries against the database for information about applications.</p> <p>Administrators: System administrators will have access for system operation monitoring and system maintenance.</p> <p>Developers: Developers for developing purposes.</p> <p>Contractors: Direct Contractors will perform data entry.</p>
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	System administrators grant access to the system based on the user's job description (role-based access). To access the system each user must submit a request for access approval. If successful, they are granted access and can only logon through single sign-on (SSO) granted through their FDA badge (PIV card).
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.	DASH uses role-based permission to limit access to appropriate PII. To access the system each user must be individually granted access and can only logon through HHS SSO granted via their FDA badge.
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.	Training includes but is not limited to annual mandatory FDA-wide information security and privacy awareness training, records management training, other role-based training, and acceptance of the HHS Rules of Behavior. Additional training is available from the FDA Privacy Office.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	A demonstration of DASH and DASH training materials includes: a concise user guide, a demonstration-style live training available as a recording, a user manual, and Frequently Asked Questions (FAQ) document that outlines the purpose and features of DASH, data collection SOPs, and a data dictionary. Additionally, live and in-person DASH demonstrations are also available.
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).	<p>Because the data in DASH consists of copies of information found in DARRTS or in publicly available resources, and DASH is a tool and not a system of record like DARRTS, records management requirements – like the need for a records control schedule – do not apply to DASH. Hence, no dedicated records control schedule applies to DASH. DASH records are maintained in accordance with NARA citation N1-088-07-2 and the specific provisions for FDA adverse event report records which provide for destruction of records 10 years after the end of the calendar year of creation or when the system becomes obsolete.</p>

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 multifactor 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:	7/15/2024
Privacy Analyst Comments:		Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	
SOP Comments:		SOP Review Date:	7/15/2024
		SOP Days Open:	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	7/19/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 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:	8/2/2024
		SAOP Days Open:	14

Supporting Document(s)				
Name	Size	Type	Upload Date	Downloads
CDER Data Analysis Search Host_SOP Approved.pdf	157662	.pdf	7/16/2024 8:14 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 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:	8/2/2024 4:35 PM	History Log:	View History Log