PTA / PIA: FDA - RAPID - QTR3 - 2025 - FDA4955769

Created Date: 8/27/2025 6:42 PM Last Updated: 9/8/2025 4:22 PM

General Information

PTA / PIA Name:	FDA - RAPID - QTR3 - 2025 - FDA4955769	**PTA / PIA ID:**	3718083
Component Name:	FDA - CDER Real World Application Platform for Innovation and Development	**ATO Boundary Name:**	CDRH Scientific and Research General Support Systems
Overall Status:	Complete	**# of Days - Open:**	13
Submitter:		**Submit Date:**	9/2/2025
Next Assessment Date:	09/07/2028	**Expiration Date:**	9/7/2028
Office:		**OpDiv:**	FDA
Security Categorization:	High		
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.	5/18/2023
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Gregory Jackson
PTA 01A:	POC Title and Organization	Program Manager FDA/OC
PTA 01B:	POC Email Address	gregory.jackson@fda.hhs.gov
PTA 01C:	POC Phone Number	301-796-4096
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	FDA has made no changes to this component since the last Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) was approved.
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 Center for Drug Evaluation and Research (CDER) Real World Application Platform for Innovation and Development (RAPID) is an entirely cloud-based, production ready system that enables the collection, storage, and analysis of real-world evidence data to advance the surveillance and analysis mission of the Food and Drug Administration (FDA). CDER RAPID leverages innovations in big data, cloud computing, containerization, security and communications to operationalize the FDA's vision for a digital platform for knowledge management. The system brings together the collective insight of medical and patient communities ("social knowledge") with ontologies, rules and logic ("unified knowledge") and enables FDA reviewers and collaborators to address product safety issues and improve patient care. The system is designed and implemented in the RAPID FDA Amazon Web Services (AWS) GovCloud Environment (the subject of a separate assessment). A multi-tenant RAPID analytics hub containing multiple analytics software platforms is available for projects (including JupyterHub, POSIT Connect, POSIT Workbench, Tableau, Analysis Studio, and Qlik Sense to analyze and visualize data in an ad hoc manner). Data is extracted from existing FDA databases (assessed separately) and ingested by RAPID for the purposes of testing the functionality of applications being built in RAPID. These research, prototypes and proof-of-concepts must be tested with real data. CDER RAPID also includes artificial intelligence (AI) capabilities which are not in use at this time. The platform utilizes AWS Console Services for monitoring itself-Cloudwatch. These tools are accessible only to system administrators as controlled by the RAPID role-based access control (RBAC) measures currently in place. System "users" consist of RAPID business owners, system administrators, development team, and internal stakeholders (all users are FDA permanent employees and Direct Contractors). Access to the RAPID homepage does not require the use of user credentials (it launches from an open website on FDA's Intranet). Users access the RAPID platform applications via FDA's single sign-on (SSO) authentication solution.

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 RAPID collects personally identifiable information (PII). The system integrates with multiple FDA systems and applications that utilize diverse data types that are stored in source systems' databases (assessed separately). Source systems provide the following patient related data to RAPID: (a) first and last name (if included in an adverse event report or materials submitted in support of a new drug product); (b) e-mail address (business and/or personal); (c) Date of Birth (DOB)/age; and (d) medical history/records. RAPID also collects PII in the form of usernames of FDA permanent employees and Direct Contractors who access the system. This information is captured and included as part of system access log records. RAPID uses LogStash to store database server/application logs, which records usernames. LogStash is accessible only by an FDA badged system administrator. PII in the system is retained on a temporary basis per National Archives Records Administration (NARA) retention and disposal schedules. The PII in the system is not shared with any other system or organization.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	Yes, but the user credentials are maintained in a separate system (e.g., Active Directory (AD), AMS) and not collected or maintained by this system. The system providing credentials is Active Directory.
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.	CDER RAPID is a secure, cloud-based platform that collects and maintains public health data to be used by FDA to make informed public health decisions and support CDER business processes. Information collected and maintained by the system is sourced from separately assessed FDA systems and/or applications, as well as system access logs (usernames only). Adverse events and drug applications related data is accessible through RAPID. PII data included with these reports includes: (a) patients' first and last name (b) e-mail address (business and/or personal); (c) patients' DOB/age; and (d) medical history/records. CDER RAPID also collects FDA employee usernames.
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://rapid.fda.gov/

PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No
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 RAPID website is to display available analytic tools, access links for analytics tools, view current projects being supported by the system, and view published articles. Only FDA permanent employees and Direct Contractors can access the system and do so via an internal uniform resource locator (URL) using SSO authentication methods.
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?	No
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 Date of Birth User Credentials Contact Information Email Address (Personal) Email Address (Business) Medical Information Medical Records Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	FDA employee and Direct Contractor username. Age.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Patients Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	<100

PIA 25:	For what primary purpose is the PII used?	The data ingested into RAPID is extracted from internal databases for the purposes of testing the functionality of applications being built in RAPID. These research, prototypes and proof-of-concepts must be tested with real data. The data does not stay in RAPID once the application is ready for production or enterprise releases.
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.	All submissions maintained in CDER RAPID are in support of FDA activities authorized by the Federal Food, Drug, and Cosmetic Act. 21 U.S.C. 301. 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.	Government Sources Within the OPDIV
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.	CDER RAPID does not collect information using an information collection request as defined by the Paperwork Reduction Act.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
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.	FDA personnel (permanent employees and Direct Contractors) are notified at the time of hire of the Agency's collection, creation, and use of their PII in the context of their work with the Agency. At every instance of logging on to the FDA network, they must read and acknowledge a warning message advising that they have no expectation of privacy when using government systems and resources. For other systems that are the source of PII in CDER RAPID, individuals may be provided additional notice in the context of those other systems. This PIA provides additional notice.

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.	No such changes are anticipated. If FDA changes its practices with regard to the collection or handling of PII related to CDER RAPID 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 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 a number of avenues available to resolve the situation. Employees may submit concerns to their supervisor, the FDA Privacy Office, a 24-hour technical assistance line, and FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). All FDA personnel are required to immediately report any suspected data breaches and security incidents to CIOCC.
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.	CDER RAPID is an entirely cloud-based, production ready system that provides the infrastructure to support innovative knowledge management. Any PII collected is stored on a temporary basis for testing purposes only. As such, source systems which provide the data are responsible for the periodic reviews of PII contained within their systems to ensure data integrity, accuracy and relevancy.
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
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: must have access to the data to evaluate the information to analyze safety of approved drugs, need for recalls, identify any public health risks. Administrators: require access to assist with data connection issues, configuration and monitor output of system. Developers: require access to the system to modify backend structures. Contractors: some administrators and developers are Direct Contractors.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and Direct Contractors with valid network accounts who require access to RAPID must have supervisor approval before access is granted. 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.	The relevant supervisor indicates on the user account creation form the minimum access that is required in order for the user to complete his/her job. The scope of access is restricted based on role-based criteria.
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 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.	Users are provided with user guides and manuals, and privacy guidance is available on the FDA intranet and from Privacy staff.
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:**	9/2/2025
Privacy Analyst Review Comments:	Note the 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. At this time, we are unable to update Archer to reflect the correct answer “Yes.” The ATO date is 5/18/2023. The FDA Archer Team is aware of this occurrence and is working on a solution.	**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	9/2/2025
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:**	9/3/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 9/3/2025 All comments have been addressed. 9/2/2025: Please see comment and update accordingly: PIA 22: Please list "Email (Personal) and Email (Business)" as PII elements that are collected, maintained, and stored, in the system. PIA-22A: Under Other, in the textbox please include "age."	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	9/8/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	5

SAOP Signature

Date	User	Type	Name	Original Value	New Value
9/8/2025 4:00 PM	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	BLAND, CRYSTAL	8/28/2025	Per FDA's Email: Note the Archer error associated with question General 03: “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” o The FDA instance of Archer is automatically entering the answer “No” which is incorrect. o At this time, we are unable to update Archer to reflect the correct answer “Yes.” The ATO dates provided for both are correct. The FDA Archer Team is aware of this occurrence and is working on a solution.	8-28-2025 EMAIL_PIA in Queue-CDER RAPID and OC Office365.pdf CDER RAPID SOP Approved8.27.25.pdf
PIA 22A	BLAND, CRYSTAL	9/2/2025	Under Other, in the textbox please include "age."	
PIA 22	BLAND, CRYSTAL	9/2/2025	Per PTA-5: Please list "Email (Personal) and Email (Business)" as PII elements that are collected, maintained, and stored, in the system.	