PTA / PIA: FDA - AWS GovCloud - QTR2 - 2025 - FDA4919119

Created Date: 5/7/2025 4:25 PM Last Updated: 5/30/2025 4:38 PM

General Information

PTA / PIA Name:	FDA - AWS GovCloud - QTR2 - 2025 - FDA4919119	**PTA / PIA ID:**	3147886
Component Name:	FDA - OC Amazon Web Services GovCloud	**ATO Boundary Name:**	
Overall Status:	Complete 	**# of Days - Open:**	31
Submitter:		**Submit Date:**	5/1/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
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?	No
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.	10/31/2022
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	Tom Vittetoe / Jon McLennan
PTA 01A:	POC Title and Organization	Tom Vittetoe - Cloud Operations Tech Lead / ODT Jon McLennan - Cloud Operation Lead / ODT
PTA 01B:	POC Email Address	tom.vittetoe@fda.hhs.gov
PTA 01C:	POC Phone Number	240 762-2220
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.	This was initially a PTA but now collects PII so now requires the completion of this PIA.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Contractor
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.	Amazon Web Services (AWS) GovCloud is the FDA's standardized configuration for AWS GovCloud Accounts that meets the Agency requirements for hosting systems rated FISMA high. The system represents the enforcement of this configuration standard using policy restrictions. The policy restrictions include prevention of using AWS Services not included in the system Authorization to Operate (ATO), compliance with FDA private network connectivity, and mandatory use of FDA Single Sign-On (SSO) and Person Identity Verification (PIV) cards for access to AWS management interfaces.
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.	The types of information collected into the system are user login id. The amount of time the PII is stored in the system is 90 days
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.	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.	The login information for Global/System and Application admins is collected and/or maintained in order to log activity and track changes to the system. PII from the system/component/collection about is shared with splunk for additional long-term storage and review.
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://sso2.fda.gov/idp/startSSO.ping?PartnerSpId=FDA_AWS_GovCloud
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.	Amazon Web Services (AWS) GovCloud is the FDA's standardized configuration for AWS GovCloud Accounts that meets the Agency requirements for hosting systems rated FISMA high. The system represents the enforcement of this configuration standard using policy restrictions. The policy restrictions include prevention of using AWS Services not included in the system ATO, compliance with FDA private network connectivity, and mandatory use of FDA Single Sign-On (SSO) and Person Identity Verification (PIV) cards for access to AWS management interfaces.

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 User Credentials
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100 – 499
PIA 25:	For what primary purpose is the PII used?	AWS logs all interactions with its management instrumentation. Actions taken by administrators are logged with the role and federated username of the administrator. The FDA Active Directory administrator's username could be inferred from these log entries.
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 legal authorities that govern information use and disclosures specific to the system and program are: Federal Information Security Modernization Act of 2014 (FISMA), Privacy Act of 2002, and the Federal Risk and Authorization Management Program (FedRAMP) Authorization Act.
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.	An OMB information collection approval number is not required. AWS does not hold information collected under the Paperwork Reduction (PRA).
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.	Notification is not provided by AWS, because the PII is not directly collected from the individual. The PII that is collected in a separate application, which is the FDA's Active Directory.
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.	Notification is not provided by AWS, because the PII is not directly collected from the individual. The PII that is collected in a separate application, which is the FDA's Active Directory.
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.	The PII data is obtained from another FDA system, therefore, there is no process in place by AWS to address an individuals' concerns. However, complaints regarding the use of a system user's PII can be sent to any of the individual AWS hosted system administrators. These complaints will be managed by the individual application teams.
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.	There is no process for periodic reviews in OC Amazon Web Services GovCloud High. This is inherited from Active Directory.
PIA 38:	Identify who will have access to the PII in the system.	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.	The reason the administrators, developers, and contractors (HHS Direct Contractors) need access to PII is to track changes within the application environment.
PIA 40:	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 governed by the Role Based Access Control (RBAC) policy. Access is role based, and system users access the minimum amount of information necessary to perform the job.
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 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. Users with access to PII can only see user id in cloudtrail logs. No other PII is visible.
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 FDA system users complete annual FDA information security and privacy awareness training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	No additional system-specific training is received by users.

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).	The following process and guidelines are in place for the retention and destruction of PII. Cloudtrail logs are only kept for 90 days before being deleted, this is an AWS policy. These records are maintained under FDA File Code 9962 (NARA GRS 20, Item 1c; superseded by the new General Records Schedule (GRS) 3.2, item 030 (DAA-GRS-2013-0006-0003), which is for “records … created as part of the user identification and authorization process to gain access to systems. " Under this schedule, retention is until "business use ceases." In other words, NARA concurs that agencies may dispose of these records as soon as they are no longer needed.
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 and implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Only users identified in an RBAC can access cloudtrail logs containing PII. 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 and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/7/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	6

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/7/2025
SOP Review Comments:		**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	5/12/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 5/12/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	5

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/30/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	18

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/30/2025 1:42 PM	GUENTHER, BRIDGET	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	5/12/2025	5/12/2025 Per FDA's Email, the ATO date for OC Amazon Web Services GovCloud is 10/20/2022.	5-12-2025 EMAIL_RE_ FDA - AWS GovCloud - QTR2 - 2025 - FDA4919119.pdf