PTA / PIA: FDA - GCPAI - QTR4 - 2025 - FDA4979362

Created Date: 10/14/2025 4:37 PM Last Updated: 12/22/2025 3:42 PM

General Information

PTA / PIA Name:	FDA - GCPAI - QTR4 - 2025 - FDA4979362	**PTA / PIA ID:**	3908052
Component Name:	FDA - OC Google Cloud Platform AI	**ATO Boundary Name:**	OC Google Cloud Platform AI
Overall Status:	Complete	**# of Days - Open:**	69
Submitter:		**Submit Date:**	11/20/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
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)?	Yes
General 04:	ATO Date or Planned ATO Date.	5/25/2025
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Sridhar Mantha
PTA 01A:	POC Title and Organization	Chief Information Officer, Food and Drug Administration (FDA)
PTA 01B:	POC Email Address	sridhar.mantha@fda.hhs.gov
PTA 01C:	POC Phone Number	(240) 760-0722
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
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	The Food and Drug Administration (FDA) plays a critical role in protecting and promoting public

those functions in support of HHS.

health. Artificial Intelligence (AI) is increasingly being used to advance public health agency activities. In alignment with Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (October 30, 2023), and Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government (December 8, 2020), the FDA Office of the Commissioner (OC) recently launched Elsa (the subject of a separate assessment), an internal-only Generative AI (GAI) tool designed to help employees work more efficiently and effectively in furtherance of the FDA's public health responsibilities. To support the Agency's advancing use of Generative AI, FDA has adopted the use of OC Google Cloud Platform AI (OC GCPAI), a suite of products from Google-controlled development environments offering users fully customizable virtual machines, databases, data analytics tools, networking services, access management tools, AI and machine learning capabilities, developer tools and other services in a secure Federal Risk and Authorization Management Program (FedRamp) platform.

OC GCPAI provides users with a high-security computing and data storage infrastructure in which to host and manage FDA systems and applications. FDA's implementation of OC GCPAI will add several resources to the Elsa GAI system that promote greater Agency efficiency and responsible secure management of data. Together with FDA's OC Google Workspace AI (the subject of a separate assessment), OC GCPAI enhances the overall Elsa user experience.

Users of the OC GCPAI system are FDA permanent employees and Direct Contractors. Use of the system is limited to Developers and Administrators (Admins). Developers will use the system to maintain and manage Elsa AI data models and workspace applications. System Admins will use the system to oversee access permissions, audit system logs, and system security.

By default, Google does not have access to customer data handled within the FDA GCPAI environment. The Google Cloud service is built on a foundation of secure infrastructure, robust access controls, and comprehensive contractual terms and conditions which govern data use and control. Collectively, all ensure that FDA data remains private and fully under FDA's control. The same security and data protections remain in place when FDA personnel use OC GCPAI in conjunction with Elsa and all data interactions (user inputs, outputs, etc.) remain confined within FDA's highly secure AI operations environment.

Access to the system is provided through an externally available uniform resource locator (URL) and network-level single sign-on (SSO) authentication methods requiring the use of an

		individual's personal identity verification card (PIV). The external URL serves as a secure gateway to the internal only FDA system. The external URL cannot be used by any unauthorized individuals or entities to access the system or the FDA network. All connections are authenticated in accordance with FDA cybersecurity policies ensuring that FDA's management the OC GCPAI environment and associated data will not be exposed to the public. OC GCPAI does not by design directly solicit, collect, or maintain personally identifiable information (PII). However, user credentials are collected and used solely for the purpose of authenticating the user against FDA's Active Directory (AD-the subject of a separate assessment). User email and username are stored in the system. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.
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.	FDA does not use OC GCPAI to collect PII or any other information directly from members of the public nor any other individuals other than internal users. The system may collect and maintain system Admin/Developer name, work email address, user credentials (username), device identifiers and job title. When used in conjunction with FDA's Elsa, PII handled in Elsa (including user inputs/outputs, derived from Elsa large learning models, library, etc.) is not handled or stored within the OC GCPAI environment. Elsa users' control and manage the information they process in Elsa independently from the OC GCPAI system. The system also collects and/or maintains the following non-PII: 1) intellectual Property (IP) addresses; 2) system/audit logs; 3) usage data (by organization); and 4) billing records. PII is not used for retrieval of records in OC GCPAI. Information in the system is stored in the system in accordance with applicable National Archives and Records Administration (NARA) records retention schedules.
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.	OC GCPAI collects a user's name, work email address, username and job title. User identification credentials are necessarily collected to allow and manage user access via SSO authentication methods and use of FDA PIV card. OC GCPAI does not share information outside the FDA. Only permanent FDA personnel and FDA Direct (PIV badged) Contractors working as authorized Admins or Developers have access to the system and data.
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://cloud.google.com/vertex-ai
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 website is to provide OC GCPAI Admins and Developers access to the system to complete testing, troubleshooting and maintenance. FDA GCPAI Admins and Developers access the website via SSO authentication methods and use of PIV card. Only GCPAI Admins and Developers can access the Google Cloud Platform Portal using a secure external URL and network access credentials.
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?	Yes

PTA 21A:	What are the AI tools and how are they used?	The following tools are available for use by FDA via OC GCPAI: Core AI/Machine Learning (ML) Services include: 1. Vertex AI - Comprehensive machine learning platform for building, deploying, and scaling ML models with pre-trained and custom model capabilities 2. AutoML - Automated ML tools for creating custom models without extensive ML expertise 3. AI Platform - End-to-end ML workflow management and model deployment services Pre-trained AI Application Programming Interfaces (APIs) 1. Vision AI - Image analysis and optical character recognition capabilities 2. Natural Language AI - Text analysis, sentiment analysis, and language understanding services 3. Translation AI - Multi-language translation capabilities 4. Speech-to-Text and Text-to-Speech - Audio processing and conversion services These tools are made available only to FDA GCPAI Admins and/or Developers for integration into specialized FDA applications.

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.	Identifying Numbers Device Identifiers Biographical Information Name User Credentials Contact Information Email Address (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	User Credentials include username only; job title.
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.	50,000 – 99,999
PIA 25:	For what primary purpose is the PII used?	The FDA uses employee PII for the primary purpose of managing system functions, operations and access. OC GCPAI logs actions taken by Developers and/or Admins. Logs include the role and federated username of the Developer and/or Admin.

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.	Title 42 of the US Code (Public Health and Welfare; HHS legal authority to operate); 21 USC 301 (Federal Food Drug and Cosmetic Act); 5 USC 301 generally authorizing agencies to establish the necessary systems and structures to operate effectively.
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.	The Paperwork Reduction Act (PRA) only requires an Office of Management and Budget (OMB) information collection approval number if the system collects information from 10 or more persons other than Federal Employees. OC Elsa collects credentialing information from Federal Employees and Direct Contractors and does not collect information on the public. As such, OC GCPAI does not require an OMB information collection approval number.
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.	There are no opt-out procedures specific to OC GCPAI because the PII is not directly collected from the individual. The PII that is collected originates from the FDA's Active Directory, which is covered by its own PIA. FDA users provide their contact information as a practical requirement in order to gain access to the source system (doing so via SSO and use of PIV card) and as a condition of employment or contract agreement.
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 OC GCPAI because the PII is not directly collected from the individual. The PII that is collected originates from the FDA's Active Directory, which is covered by another PIA. In the event of a major change to the source system, the FDA's Active Directory team will notify system users of the change and obtain feedback. If FDA changes its practices with regard to the collection or handling of PII related to the website, 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 email to individuals, adding or updating online notices or forms, updating this assessment, 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.	There is no process in place for OC GCPAI to address an individuals' concerns as the PII data is obtained from a different FDA system. However, complaints regarding the use of a system user's PII can be sent to any of the individual Google Cloud Platform hosted applications system Admins. An individual may also contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and other agency offices, via email, phone, and standard mail (all listed on fda.gov and the FDA intranet). Regardless of the system, in the event of a suspected incident or data breach, FDA personnel must immediately report this information without delay to the FDA's 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.	There is no process for periodic reviews of PII in OC GCPAI. The data originates from and is reviewed by FDA's Active Directory and follows processes established by that system. FDA's Office of Information Security (OIS) performs user account validation quarterly. As part of this exercise, each account is validated for accuracy and the correct permission levels. Individuals voluntarily provide their PII. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. PII relevancy is supported through the design of the system to require and collect only the PII elements necessary to administer the system and enable its intended use. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Integrity and availability are protected by privacy and security controls selected and implemented in the course of providing the system with an authorization to operate (ATO). Controls are selected based on National Institute of Standards and Technology (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.
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.	Admins require access to verify users in the system. Developers require access to analyze usage data. Contractors help with both administration and development. Some Admins 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.	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. The relevant supervisor will indicate the minimum access that is required in order for the user to complete his or her 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 scope of access is restricted based on role-based criteria using network and system level controls and settings to control access at the individual level. System Admins and Developers require access to account information in order to access usage data and manage and maintain the system. Users with access to PII can only see user identifiers in audit logs. No other PII is visible There is minimal PII contained in OC GCPAI.
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 Digital Transformation (ODT) verifies that training has been successfully completed.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Personnel are trained on the use of the system and review the Rules of Behavior. Additional role-based training on privacy is available via FDA's privacy office.

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).	General Records Schedule (GRS) 3.2: Information Systems Security Records, Item 030, System Access Records. Temporary. Destroy when business use ceases. Systems Requiring Special Accountability for Access. Temporary. Audit log files may be held for 6 years but longer retention is authorized if required for business use. General Records Schedule (GRS) 3.1: General Technology Management Records. 010, Information technology development project records. Destroy 5 years after project is terminated, but longer retention is authorized if required for business use. General Records Schedule (GRS) 3.1: General Technology Management Records. 011, System development records. Destroy 5 years after project is terminated, 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.	OC GCPAI utilizes SSO for authentication purposes, which requires use of the FDA issued PIV card. OC GCPAI limits access to data to only those that have explicitly been granted access. Administrative safeguards include user training and implementation of Need to Know and Minimum Necessary principles when awarding access. Only users identified in an RBAC can access OC GCPAI 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:**	11/20/2025
Privacy Analyst Review Comments:	Requested update completed. PIA is ready for review.	**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	11/20/2025
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:**	12/18/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 12/18/2025 Comments have been addressed and AI review completed. This PIA is ready for SAOP review and approval. 11/19/2025 Please see comment and update accordingly: PTA-4: Please include the following AI statement at the end of your response: "The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks."	**# of Days - APA Review:**	28

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	12/22/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	4

SAOP Signature

Date	User	Type	Name	Original Value	New Value
12/22/2025 1:04 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 04	BLAND, CRYSTAL	11/19/2025	Please include the following AI statement at the end of your response: "The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks."	
PTA 21A	BLAND, CRYSTAL	12/18/2025	12/18/2025 AI Review Completed.	12-18-2025 CDC_FDA_RE_ AI Review Status_complete.pdf