PTA / PIA: FDA - Elsa - QTR3 - 2025 - FDA4972357

Created Date: 9/25/2025 4:37 PM Last Updated: 9/26/2025 12:36 PM

General Information

PTA / PIA Name:	FDA - Elsa - QTR3 - 2025 - FDA4972357	**PTA / PIA ID:**	3863838
Component Name:	FDA - OC Elsa	**ATO Boundary Name:**	OC HALO
Overall Status:	Complete	**# of Days - Open:**	3
Submitter:		**Submit Date:**	9/25/2025
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.	Initiation
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.	5/22/2025
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	Venu Boppana
PTA 01A:	POC Title and Organization	Senior Operations Research CDER/Office of Strategic Programs (OSP)/Office of Business Informatics (OBI)
PTA 01B:	POC Email Address	venugopal.boppana@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-0977
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 those functions in support of HHS.	Artificial Intelligence (AI) offers the Food and Drug Administration (FDA) powerful tools to analyze data, streamline regulatory reviews and support the Agency's overall mission to protect public health. In accordance 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) has launched Elsa, a generative Artificial Intelligence ("Gen AI," a class of AI models)) tool designed to modernize agency workflows and important regulatory review processes. The purpose of OC Elsa is to help employees work more efficiently and effectively in furtherance of the FDA's public health responsibilities. It is employed as a work-assisting tool and not a vehicle to solicit or collect information. Users of this enterprise-wide tool are limited to FDA permanent employees and Direct Contractors. Using OC Elsa, users can quickly synthesize and summarize large, complex data sets enabling faster and more efficient decision-making. The system is also used by FDA personnel to enhance written communications and ease document review. OC Elsa employs foundational large language models (LLMs) to generate dynamic, personalized responses based on user prompts. The LLMs in use at the time of this assessment include pre-trained static versions of Claude Sonnet, Gemini, and Titan Embeddings. All LLM use occurs within the confines of FDA Elsa. OC Elsa is operated and maintained by FDA, in an FDA high-security controlled GovCloud environment. There is no third-party access to the system. Users have the capability to create their own personal workspaces, to include personalized document collections based on project and work streams. Although OC Elsa is designed to assist in informing Agency actions and decisions, it does not independently determine final outcomes. All decisions will be subject to human oversight and made by authorized FDA personnel. OC Elsa does not provide access to any internal FDA databases or any real-time FDA systems; the system does not directly access or draw data from other internal FDA systems and does not enable users to access other systems through Elsa. Users control what materials are in Elsa through their chosen interactions with Elsa in performing their work. OC Elsa offers two distinct modes of user interaction. The first is a general chat feature that relies on general publicly available knowledge to assist users and answer questions. Publicly available knowledge refers to generalized

		knowledge and information available via the employed LLMs. No FDA data is used to train the LLMs. The second mode of user interaction is a document library chat feature that provides users with a more personalized experience, completing targeted searches through specific FDA documents and files before combining FDA information with OC Elsa's general knowledge to provide the user with customized responses. User-created document libraries reside in Elsa where personnel can use Elsa to analyze library content. Outside of document libraries, they can also upload documents for analysis when submitting prompts through the chat feature. If FDA decides to integrate OC Elsa with other FDA systems/components, responsible System Owner(s) will update this and/or other privacy impact assessment (PIA) prior to implementing integrations that involve major changes or other steps which alter the privacy risks associated with the system. OC Elsa is hosted in a secure, FDA-approved cloud environment, located behind an FDA firewall. Users access this internal-only system using network-level single sign-on (SSO) authentication methods requiring the use of an individual's personal identity verification card (PIV). OC ELSA also includes a secure mobile web interface that users can access on their FDA-issued mobile devices using client certificates (rather than PIV card credential verification).
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 majority of information collected or introduced into Elsa by users is non-personally identifiable information (PII) including: 1) User prompt messages; 2) Extracted text content from user uploaded documents; and 3) Large language model (LLM) response messages. The Elsa system collects only each user's name, work email address, and user credentials (username only). FDA does not use the system to collect PII or any other information directly from members of the public nor any other individuals other than internal Elsa users. FDA does not use Elsa in a public-facing way. There are no external users; no individuals outside FDA are permitted access to Elsa, including personnel in partner agencies or organizations. In order to effectively use Elsa to assist in their work, users are permitted to include non-public information contained in materials used for their authorized duties performed with the assistance of Elsa. Inputs could potentially include PII about anyone and any other information into Elsa, such as within a prompt/chat entry, within a document uploaded in the context of a prompt, or as contained in a document library within Elsa. However, neither the functionality of Elsa nor the data entered in Elsa is used for the purpose of

		identifying individuals. The system maintains all user prompts and text extracted from uploaded documents which may include business related and/or non-public information and potentially PII (although that is not the intended or expected use of Elsa). All documents, document libraries, chats/prompts and generated output from Elsa's AI analysis in response to prompts is maintained in Elsa in accordance with applicable records schedules. Information use, sharing and disclosure: Users control the information that is entered into and maintained in Elsa and the sharing and disclosure of Elsa information. They must adhere to the Department of Health and Human Services (HHS) Rules of Behavior, and to the laws and policies that apply to their work and to the information they handle while performing their duties. To the extent that information in Elsa constitutes a federal record, users are responsible for recognizing this and following the appropriate schedule. Users are responsible for adhering to information use and disclosure laws and policies. Users must ensure that when inputting information from other FDA systems and information collections into Elsa, the information use, disclosure, and privacy and security controls that apply in the context of the source system are maintained and applied in the context of Elsa. Individual user prompts, document uploads and chat output/system interaction information is not accessible to other users. Libraries are accessible only to individuals and groups expressly permitted access by the library owner. Individual users may establish their own libraries and are responsible for ensuring appropriate access permissions. At system login prior to accessing OC Elsa, users are required to acknowledge there is no expectation of personal privacy when using FDA-authorized generative AI tools and that all uses must be exclusively for official FDA business purposes.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Username

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.	Elsa is not employed for the purpose of collecting PII. The primary purpose for the collection of the limited user PII collected into Elsa is to manage system functions, operations and access. User identification credentials are necessarily collected in Elsa to allow and manage user access via single sign-on (SSO) authentication methods and use of FDA PIV card. To enable effective use of Elsa to strengthen and modernize internal FDA activities at all levels, users are permitted to bring any type of information into Elsa when performing their work. Information users input and the response to their prompts is maintained in Elsa, to include user prompt messages, extracted text content from user uploaded documents, and large language model (LLM) response messages. This information is maintained in Elsa to allow user work continuity and avoid duplicative work. Elsa does not provide the ability to share information outside the FDA.
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).	HHS Internal Only: https://elsa.fda.gov/elsa/
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 website serves as a front-end for users to interface with OC Elsa LLM. Users (FDA permanent employees and Direct Contractors) access the website via an internal only uniform resource locator (URL): https://elsa.fda.gov/elsa/. Users may also access Elsa using their FDA issued mobile device using the available browser on their phone and authenticate through client certificates.
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?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies- Collects PII
PTA 12C:	What PII is collected by the web measurement and customization technology?	Name and email address.
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 product is a chatbot (Generative AI). It uses foundational LLMs. FDA employs Elsa to respond to user chat queries, accept documents, assist users with drafting content, researching, summarizing, learning, and analyzing information and documents in the course of the internal FDA work.

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 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.	Potential PII contained within a chat prompt, in documents entered into Elsa, or that is produced in response to a prompt.
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.	10,000 – 49,999
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. User identification credentials are necessarily collected in Elsa to allow and manage user access via single sign-on (SSO) authentication methods and use of FDA identity verification (PIV) card. Aggregate data rather than user PII is used when analyzing system use and support needs.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	None.
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.	Directly from an individual about whom the information pertains Online
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 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 Elsa 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.	FDA users provide their contact information as a practical requirement in order to gain access to the system (doing so via SSO and PIV) and as a condition of employment or contract agreement. There are no opt-out procedures specific to OC Elsa.
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.	In the event of a major change to the system, the OC Elsa 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.	If the system contains incorrect contact information for a user, the account likely will not function properly and system administrators would fix the issue. If a user notices incorrect information in their account, the user can contact system administrators to fix it. Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA system have many avenues available for assistance. Individuals may 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 avenues (all listed on fda.gov and the FDA intranet). 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.	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.	The reason the following groups need access to PII is: - Administrators need to be able to verify users in the system. - Developers need to be able to analyze usage data. - Contractors help with both administration and development. Some administrators are contractors.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA Employees and Direct Contractors with valid network accounts who require access to the system must obtain supervisory approval and signature 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. Access is confined to a small group and evaluated on a request basis to project leads.

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.	System administrators and developers require access to account information in order to access usage data, and manage and maintain the system. There is minimal PII contained in OC Elsa. The relevant supervisor will indicate 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 using network and system level controls and settings to control access at the individual level.
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.	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).	FDA currently maintains Elsa records as noted below or indefinitely pending schedule assessment. Systems Requiring Special Accountability for Access. TEMPORARY. Audit log files may be held for 6 years. General Records Schedule (GRS) 3.2: Information Systems Security Records. 030, System access records. Temporary. Destroy when business use ceases. 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 Elsa utilizes SSO for authentication purposes, which requires use of a personal identity verification (PIV) card issued by the FDA. OC Elsa limits access to data to only those that have explicitly been granted access. 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 and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	9/25/2025
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 5/22/2025. 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:**	9/25/2025
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:**	9/26/2025
Agency Privacy Analyst Review Comments:	Ready for SAOP review - Nestor Villafuerte	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	9/26/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
9/26/2025 9:33 AM	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	VILLAFUERTE, NESTOR	9/26/2025	Per FDA: “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 5/22/2025. The FDA Archer Team is aware of this occurrence and is working on a solution.	