Privacy Impact Assessment (PIA): FDA - GSRS - QTR1 - 2025 - FDA4900646

Created Date: 1/8/2025 3:26 PM Last Updated: 2/11/2025 3:32 PM

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 - GSRS - QTR1 - 2025 - FDA4900646	**PIA ID:**	2622365
Name of Component:	FDA - OC Global Substance Registration System	**Name of ATO Boundary:**	CDRH Scientific and Research General Support Systems
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	34
Submission Status:	Submitted	**Submit Date:**	1/8/2025
Next Assessment Date:	N/A	**Expiration Date:**	2/11/2028
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4900646
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)?	No
4:	ATO Date or Planned ATO Date.	1/31/2023
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.	Since the last approved Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) there have been no changes to the Global Substance Registration System (GSRS).
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.	The purpose of the Office of the Commissioner (OC) Global Substance Registration System (GSRS) is to enable the Food and Drug Administration (FDA) to efficiently, effectively and reliably define all substances of interest to the FDA (regulated drugs, biologics, foods, and devices) and provide a reliable Unique Ingredient Identifier (UNII) code for these substances. OC GSRS maintains compliance with the International Organization for Standardization (ISO) 11238 standard, which addresses the identification and exchange of regulated information on substances. The system registers substances and generates, maintains, and disseminates UNIIs for FDA-regulated products and makes them available for use internally and in health information systems in a manner that is meaningful and consistent. The system is both upstream and downstream from other FDA systems. System users consist of internal FDA permanent employees, Direct Contractors, and possibly Fellows, Interns, or other special government employees.
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.	OC GSRS is the agency-wide substance database that contains molecular structures, substance names, and codes. It links substances to other FDA systems (addressed in separate PIAs) containing a product, clinical trial, and adverse event information. This linkage is designed so as to prevent access to personally identifiable information (PII) in those systems. Publicly available journal articles displaying author name(s), work address, and email are also stored on the file system of GSRS as references. The system captures the login identification (ID) of FDA employees and Direct Contractors who query, create or edit substances. The login ID is in the form of first and the last name pulled from FDA's Active Directory (AD). Access to the system uses a single sign-on (SSO) approach employing multi-factor authentication; there are no system-specific authentication credentials housed in the system other than the login ID used to identify the FDA user creating or editing substances in the OC GSRS database. System users are FDA employees (permanent and Direct Contractors), and may also include Fellows, Interns, or other special government employees. The system contains PII relevant to user access credentials. The FDA does not use any PII to retrieve records in the system and system capabilities do not allow for such a retrieval.
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.	HHS User Credentials HHS/OpDiv PIV Card

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.	OC GSRS is an internal web-based substance registration system. Access is controlled by SSO using role and group-based access controls. OC GSRS captures and stores information including molecular structures, substance names, and codes for the substances. Substances (e.g., chemicals, polymers, nucleic acids, proteins) are defined by their molecular structures. Substances can have many names which are decoded by using the structure. The system associates substances with relevant product, clinical trial, and adverse event information maintained in other FDA systems (each assessed separately in system specific dedicated PIAs). Additionally, all substances are shared by many different scientific communities, therefore OC GSRS attempts to reference many sources, and codes each source in order to provide a centralized repository of all information related to a particular substance. Publicly available journal articles displaying author name(s), work address, and email are also stored on the file system of OC GSRS as references. Users accessing OC GSRS are not able to search the database using any information about the author of an article. Users are only able to search the database by substance. System users consist of FDA permanent employees and Direct Contractors. Other users may include Fellows, Interns, or other special government employees. The system uses PII associated with their access credentials as provided by FDA's AD. OC GSRS maintains the login ID of FDA employees, Direct Contractors and others identified who query, create or edit substances.
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?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
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.	The purpose of the website is to both collect substance information and make it available to FDA users. Only internal users of the system can access the website via FDA's Virtual Private Network (VPN) after they are provided access by the system administrator. The website is not publicly accessible.
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 - 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?	No
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?	No

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 Mailing Address User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	51 - 200
PIA - 4:	For what primary purpose is the PII used?	The FDA uses PII (login ID-user name) for the primary purpose of identifying users creating, editing or querying records. Name of authors of publicly available journal articles in the system is captured in association with the articles.
PIA - 5:	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 - 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.	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. In addition, the security and privacy measures of the system are required by the Federal Information Security Modernization Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.
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.	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.	An OMB information collection approval number is not required as there are no forms in use and the collection is not subject to Paperwork Reduction Act (PRA) collection requirements.
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.	Submission of PII is voluntary as that term is used in the Privacy Act. The submission of PII is necessary in order for users to access and use the system. System users are employees (which may include permanent, Direct Contractors, Fellows, Interns, or other special government employees) and the system contains PII relevant to their access credentials. There is no method for employees to opt not to submit PII if they wish to access OC GSRS. Employees must provide their PII in order for the agency to process administrative materials and securely administer access to agency information and property.
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.	No such changes are anticipated. If the agency changes the collection, use, or sharing of PII data in this system, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on the FDA intranet site or an e-mail notice to the individuals. OC GSRS is SSO enabled, none of the supporting files for the substances in OC GSRS contain the usernames of users. System users/Administrators (which may include Direct Contractors, Fellows, Interns, or other special government employees) are required to provide PII to access the system; any changes in the use of their PII/user credentials will require notifying them by phone, email, and/or notices on FDA intranet.
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 who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have a number of avenues available to request to rectify the situation. FDA personnel (consisting of FDA permanent employees, Direct Contractors, Fellows, Interns, and other special government employees) may raise concerns by contacting any of the following: the OC GSRS Project Manager, FDA Contracting Officer Representative (COR); OC GSRS administration support (all reports of PII disclosure will be reviewed and processed per FDA and HHS guidelines and federal requirements; the FDA Employee Resource and Information Center (ERIC), FDA's Cybersecurity and Infrastructure Operations Coordinating Center (CIOCC) and/or Privacy Office. All personnel must rapidly report actual and suspected security incidents and data breaches to the CIOCC. Resources providing guidance on reportable events and the reporting process is provided on FDA intranet pages and in training.

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.	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. FDA systems that are the source of PII in OC GSRS have dedicated processes to support PII accuracy. 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 the 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. FDA also performs quarterly reviews to evaluate user access needs and remove instances of unnecessary access (e.g., remove accounts for retired employees).
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.	Users: Documents, such as journal articles, may contain names and may be viewed by users when reviewing. Administrators: names and login ID may be viewed by administrators when troubleshooting technical issues with system access; account management and access control. Developer: requires access for troubleshooting and system development. Contractors: Some of the administrators and developers are Direct Contractors.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	All access to the system for users, administrators, developers and Direct Contractors requires supervisory approval prior to the user gaining access. System access is reviewed on a quarterly basis to identify and remove unnecessary accounts. Users (typically query-only) need to access substances for research and review of applications and products regulated by the FDA. Administrators need to access user management, audit logs, and data management functions to support OC GSRS functionality. Developers need access to provide operations and maintenance support, data migration troubleshooting, and defect investigation. Direct Contractors provide operations and maintenance support by serving as the developers and administrators of the application.
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.	Management establishes roles for individual personnel, with role-based restrictions permitting access only to information that is required for each individual to perform his or her job.
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.	The FDA requires all agency personnel and Direct Contractors to complete FDA's Information Technology (IT) Security and Privacy Awareness training at least once every 12 months. A portion of this training is dedicated to guidance on recognizing and safeguarding PII. Completion is tracked by the Office of Digital Transformation.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Additional on-the-job or informal training may be received.
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).	Retention and destruction of PII is governed by General Records Schedule (GRS) 3.2. Item 030, System access records. Disposition Authority: DAA-GRS-2013-0006-0003. Temporary. PII is to be destroyed when business use ceases.
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 uses of firewalls; access controls such as user names; and regular testing of IT systems. 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 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:**	1/8/2025
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP 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.	**SOP Review Date:**	1/8/2025
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	1/16/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 1/16/2025 Comment about the ATO has been addressed (see email in Supporting Documentation). This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	8

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Per FDA email, Archer error for FDA - GSRS - QTR1 - 2025 - FDA4900646. The response to Q3 as entered was and should be "Yes" and the ATO date provided in Q4 is 1/31/2023.	**SAOP Review Date:**	2/11/2025
		SAOP Days Open:	26

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
1-16-2024 EMAIL_RE_ FDA PIAs_ FDA - GSRS - QTR1 - 2025 - FDA4900646.pdf	318778	.pdf	1/16/2025 2:36 PM	0
1-8-2025 OC Global Substance.pdf	168325	.pdf	1/8/2025 4:24 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	VILLAFUERTE, NESTOR	1/13/2025	Reviewer notes that the ATO date stated has passed, however, the system still indicates that it doesn't have a SA.	
PIA - 1	BLAND, CRYSTAL	1/16/2025	Per FDA email, Archer error for **FDA - GSRS - QTR1 - 2025 - FDA4900646**. The response to Q3 as entered was and should be “Yes” and the ATO date provided in Q4 is 1/31/2023.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP 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:	2/11/2025 3:32 PM	**History Log:**	View History Log