PTA / PIA: FDA - OTCM - QTR2 - 2025 - FDA4941365

Created Date: 6/11/2025 8:40 AM Last Updated: 6/23/2025 4:46 PM

General Information

PTA / PIA Name:	FDA - OTCM - QTR2 - 2025 - FDA4941365	**PTA / PIA ID:**	3307057
Component Name:	FDA - CDER Over-The-Counter Monograph	**ATO Boundary Name:**	CDER Division of Online Communication Applications
Overall Status:	Complete	**# of Days - Open:**	13
Submitter:		**Submit Date:**	6/23/2025
Next Assessment Date:	06/22/2028	**Expiration Date:**	6/22/2028
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.	9/8/2023
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	Athena Shry
PTA 01A:	POC Title and Organization	Operations Research Analyst/Office of Business Informatics
PTA 01B:	POC Email Address	athena.shry@fda.hhs.gov
PTA 01C:	POC Phone Number	Not available
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.	The Food and Drug Administration's (FDA's) Center for Drug Evaluation and Research (CDER) regulates nonprescription drugs to help ensure that they are safe and effective for their intended use. One of the ways an over the counter (OTC) drug is brought to market in the United States is via the OTC Monograph Process. Under this process, an OTC monograph is a “rule book” which establishes conditions, such as active ingredients, uses (indications), doses, labeling, and testing under which an OTC drug is generally recognized as safe and effective (GRASE). On March 27, 2020, H.R. 748, the “Coronavirus Aid, Relief, and Economic Security Act” (CARES Act) was signed into law. The law replaces the rulemaking process in the OTC Drug Review with a streamlined administrative order process to add, remove, or change GRASE conditions for an OTC drug monograph. It also establishes an expedited process to address safety issues. The subject of this assessment is the CDER Over-the-Counter Monograph (OTCM) system. CDER OTCM allows industry requestors to request a Monograph File (MGF) number (a unique identifier used to track and manage specific documents or guidelines related to a particular substance or drug) and begin multiple types of submissions to the FDA including a Meeting Request or an OTC Monograph Order Request (OMOR). Requestors may also attach documents to their submission within the OTCM use case. CDER OTCM consists of an external portal and internal module. Users of the external portal include members of the public (e.g., industry point of contacts) and access does not require a system account. The internal module is utilized by current CDER employees (FDA permanent employees and Direct Contractors) serving as system Administrators (Admins), Team Leads, or Reviewers. Access to the internal module requires an account and use of username, password, and Data Universal Numbering System (DUNS). Multifactor authentication/single sign-on (SSO) is used during every sign on attempt.

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 OTCM collects and maintains the following personally identifiable information (PII) about members of the public (e.g., industry point of contacts): (1) Name; (2) Business Address; (3) Business Email Address; (4) Business phone number/fax number; (5) Professional Credentials certifications and job title); and DUNS I.D. Number. Submissions made by members of the public may include electronic documents which may contain sensitive comments and data that require redaction during the review stage before they are published to the public-facing portal. CDER OTCM also collects and maintains the names, usernames and passwords of CDER employees. Non-PII collected and maintained by the system includes: (1) File Purpose data; (2) Meeting requests (includes meeting request type, preferred meeting format, submission contents, purpose of meeting, topics, cross reference applications, facility addresses and applicable OTC monographs); (3) OTC Monograph Order Requests (OMOR data includes OMOR classification, applicable OTC Monographs, facility addresses, study reports including study ID, title, and type); (4) Withdraw requests/records; (5) General information; (6) Information requests/responses; and (7) File over protest submissions. PII is stored in the system per National Archives and Records Administration (NARA) general record schedules (GRS), to be stored on a temporary basis or until business use ceases. PII is not used to retrieve records from the system.
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 Password

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 OTCM collects comments and other data submitted by the public and publishes OTC Monograph information and public comments to the public-facing portal so the public can view up-to-date information about proposed or final orders. Access to the public-facing portal is open to the public with no user account required. As part of the public comments, public users can voluntarily provide PII such as their contact information which may be used by internal users for the sole purpose of contacting the public user to clarify comments during the review period. Contact information includes: first and last name, business mailing address, business email address, business phone and fax number. Comments may also include sensitive comments and data that require redaction before they are published to the public facing portal. PII is not used to retrieve records held in the system. When an FDA user accesses the internal OTC monograph drug user fee program (OMUFA) module, the system automatically checks for a valid FDA network account through SSO. OMUFA stores an access control list of CDER users consisting of the username and user roles. Only active users can access the internal OMUFA module. The OMUFA internal module is utilized by CDER employees only. There are three roles within the internal OMUFA module: Admins (who manage system access and use; orders, and comments); Team Leads (who manage orders and comments); and Reviewers (who view orders and redact comments as necessary before being published to the public facing portal).
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://dps.fda.gov/omuf (public use) dps-admin.fda.gov (internal Admin use)
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes
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 public website allows any public user with the public uniform resource locator (URL) to view information about proposed/final orders published by the FDA and submit comments related to proposed orders. PII, if provided with the order comments, may be used by internal FDA personnel to contact individuals regarding their comments associated with the proposed OTC monograph order.
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?	Yes
PTA 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes
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.	Identifying Numbers DUNS Biographical Information Name User Credentials Certificates (e.g., training certificates) Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	business fax number; job title; username/password.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	PII is used for follow-up business communications with points of contact.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	N/A. FDA does not use PII for any secondary uses.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 U.S.C. 301; 21 USC 355: Regulation of certain nonprescription drugs that are marketed without an approved drug application.
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 In-person Hard Copy Mail/Fax Email Online Government Sources Within the OPDIV Non-Government Sources Members of the Public Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	OMB Control Number 0910-0340- Expires 2/28/26 OMB control number 0910-0805- Expires 3/31/2028
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	Department of Health and Human Services (HHS). The PII is shared because it is needed for the regulatory review established by OMUFA.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	As an agency within HHS, the sharing of this information by FDA with HHS is a standard part of overall departmental operations and the OMUFA process. Additionally, 21 USC 355 does not explicitly prohibit the sharing of this information between FDA and HHS.
PIA 32D:	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.	As PII information is provided by users on a voluntary basis, there are currently no procedures in place for logging/tracking such information when submitted. However, any and all submissions which do include PII are collected and maintained in accordance with current federal privacy laws and HHS regulations and policies.
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 is no option to object to or opt-out of the information collection available for internal users of the system because PII is needed for account creation. Members of the public provide PII on a voluntary basis only.

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 at this time. However, if registered account holders need to be contacted regarding changes to the system and use of their PII, affected individuals will be notified in the most efficient and effective manner available and appropriate, which may include email.
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 believe their PII has been inappropriately obtained, used or disclosed may seek assistance by contacting the OTCM Support help desk, the FDA Privacy Office, the Employee Resource and Information Center (ERIC-internal personnel only), or the Cybersecurity Infrastructure Operations Coordination Center (CIOCC). Additional information can be found on FDA.GOV or FDA Intranet pages. In the event of a suspected breach individuals are to promptly report that 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.	Each submission is viewed for only validity of submitted files and required fields. Users are not obligated to update PII. To update accuracy/relevancy of PII, users can leverage Salesforce Helpdesk to make updates. Updates to submissions in the OTCM use case is not permitted.
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: may have access to PII when reviewing submissions made by the public. Administrators: require access to monitor the system and manage system access; assist users unable to submit reviews/reports; and troubleshoot system issues. Developers: require access to manage database updates. Direct Contractors: some administrators/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 CDER OTCM must have 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.
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.	Role-based restrictions (based on team role and assigned role in CDER OTCM) are employed via technical methods to ensure system/PII access is limited to individuals who require access to perform necessary job duties. Permissions are granted where least privilege principles are enforced.
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 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 (to include any special restriction on data use and/or disclosure). The FDA Office of Digital Transformation (ODT) verifies and documents that training has been successfully completed.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	In addition to FDA mandatory training, all CDER OTCM users receive new user training, and review of standard operating procedure documentation for information on dealing with PII.

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 CDER OMUFA Publishing Platform acknowledges the Records Management Team's documentation for operating procedures for incorporating records management into processes. (Document: "CDER SOP for Incorporating RM into SOPs"). Record types and disposition follow specific record series titles for the dps.fda.gov/omufa website pages for content and data, which fall into four categories: Content pages: Include news, annual forecast, resource pages of static web page content and list of URLs. Follow: FDA-3413: Public Affairs product production files with disposition as temporary (Destroy when no longer needed for business use.) FDA-3410: Press Releases/Talk Papers for Permanent- 7 years (After 7 years is transferred to NARA per the disposition schedule.) For the comments section of the website and contact, fall into two types as structured data: FDA-3421- Public Correspondence and Communications not requiring formal action 90 days (longer retention authorized) FDA-3466b: Information Services Files. Public Customer Service Operations Records - Temporary (1 year after no longer needed for business use or issue resolved). Data in the form of OTC Monograph information and documentation is based on office management or website record type: FDA-1725- Final Grant and Cooperative Agreement Products or Deliverables (Temporary, destroy when business use ceases).
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 System Administrator control of logical access to the data; implementation of need to know and minimum necessary principles when awarding access. Technical controls protecting PII include virtual private network (VPN) and multi-factor authentication for network and system access. Physical controls applied include a keypad activated alarm system, layers of physical cage enclosures with key locks, motion detectors and video surveillance with barriers requiring personal identity verification (PIV) card authentication to gain physical access.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	6/23/2025
Privacy Analyst Review Comments:	The FDA instance of Archer is automatically entering the answer “No,” which is incorrect. The ATO date is 9/8/2023. At this time, we are unable to update Archer to reflect the correct answer “Yes.”	**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/23/2025
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:**	6/23/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/23/2025 Addressed comment. This PIA is ready for SAOP review and approval. 6/13/2025 Please see comment and update accordingly. PTA-11: This response should be "Yes" the website contains link to Facebook, X, LinkedIn, and YouTube.	**# of Days - APA Review:**	0

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/23/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/23/2025 3:11 PM	BLAND, CRYSTAL	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	6/12/2025	Per FDA's Email, Please be advised that the FDA instance of Archer is automatically generating a “No” response to general question 3. At this time, we are unable to update Archer to reflect the correct response “YES.” The ATO date is 9/8/2023.	CDER OTCM SOP approved PIA 2025.pdf 6-12-2025 EMAIL_PIA in Queue (FDA - OTCM - QTR2 - 2025 - FDA4941365 (CDER OTCM)).pdf
PTA 01C	BLAND, CRYSTAL	6/13/2025	Look in our directory and Athena Shry doesn't have a phone number. You can only reach her via email or chat.	
PTA 11	BLAND, CRYSTAL	6/13/2025	This response should be "Yes" the website contain links to Facebook, X, LinkedIn, and YouTube.	