PTA / PIA: FDA - E-Pub-C - QTR2 - 2025 - FDA4941570

Created Date: 6/18/2025 8:42 PM Last Updated: 6/27/2025 4:45 PM

General Information

PTA / PIA Name:	FDA - E-Pub-C - QTR2 - 2025 - FDA4941570	**PTA / PIA ID:**	3354762
Component Name:	FDA - HFP Electronic Publications-C	**ATO Boundary Name:**	CDRH Scientific and Research General Support Systems
Overall Status:	Complete	**# of Days - Open:**	9
Submitter:		**Submit Date:**	6/27/2025
Next Assessment Date:	06/26/2028	**Expiration Date:**	6/26/2028
Office:		**OpDiv:**	FDA
Security Categorization:	Low		
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)?	Yes
General 04:	ATO Date or Planned ATO Date.	5/29/2025
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	Claudia Lam
PTA 01A:	POC Title and Organization	Project Manager, HFP/ORM/DITM/SCISB
PTA 01B:	POC Email Address	claudia.lam@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-5431
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	FDA has made no changes to EPUB since the last Privacy Threshold Analysis/Privacy Impact Assessment was approved.

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 purpose(s) of the EPUB system is to provide an electronic publication catalog to the public. The system maintains the following non-PII data relative to each publication within the catalog: (a) publication title, (b) publication code, (c) publication description, (d) language, € downloadable, (f) hard copy availability, (g) maximum order quantity, and (h)available stock quantities. Since ePub allows public users to submit requests for hard copies of a publication, FDA also collects and maintains order data. The system generates and maintains the following non-PII data as part of this process: (a) Order ID, (b), Order Date, (c) Order Details (includes publication title and publication code), and (d) Order Quantity. The system does not have any relationship to other FDA systems. The key functional elements of the system include: Publication Catalog, Catalog Filters, Catalog Search, Publication Downloads, and Publication Hard Copy Orders. System “users” consist of the public and system administrators who manage the content provided through the catalog as well as coordinate and validate hard copy order requests with the HHS Warehouse system.
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.	Epub has two components: an external public-facing ePublication Online Ordering System (extranet) component that is open and accessible to the public, and an internal ePublication Administrator System (Intranet) component that is accessed by FDA employees and direct contractors. The EPublication Online Ordering system (external component) provides the public with the ability to browse through CFSAN’s Education Resource Library containing a catalog of printable educational materials and videos on topics related to food safety, nutrition (including labeling and dietary supplements), and cosmetics. Materials are available in PDF format for immediate download. Some print materials are also available and can be ordered individually or in limited quantities. No financial or payment data is collected by the system. User names and passwords are not created to access or submit orders in the system. In order to provide an electronic publication catalog to the public, the ePublication system maintains the following non-PII data relative to each publication within the catalog: (a) publication title, (b) publication code, (c) publication description, (d) language, € downloadable, (f) hard copy availability, (g) maximum order quantity, and (h)available stock

quantities.

Since ePub allows public users to submit requests for hard copies of a publication, FDA also collects and maintains order data. The system generates and maintains the following non-PII data as part of this process: (a) Order ID, (b), Order Date, (c) Order Details (includes publication title and publication code), and (d) Order Quantity.

The system collects the following PII data as part of this process: (a) First Name, (b) Last Name, (c), Business Street Address (d), Business Zip Code, (e) Business State, (f) Contact Details (either Business Email or Business Phone Number), and (g) Audience Type. The Epub ePub system only collects this data so that the print copies requested by the user can be shipped to their annotated shipment location. The system displays guidance on the Customer Details screen directing users to provide their business information. This data is shared / sent to the Department of Health and Human Services (HHS) document warehouse where the order is fulfilled, and the requested publication is shipped to the requestor. Only authorized FDA employees, DHHS employees, and Ddirect Ccontractors (internal users), . who require access to perform their authorized duties can access this PII in the event that an order needs to be regenerated or a follow up with the requestor is required. EPub ePub does not collect any other personal data.

The eEPublication Administrator System is the (internal component) which includes an intranet interface (intranet page) and provides FDA CFSAN's Office of Analytics and Outreach (OAO) ePublication administrator team with system administrative functions for maintaining the publication catalog. This system is only used by authorized FDA employees and direct contractors. These authorized users can access the system via a network-level Single Sign On (SSO) and multi-factor authentication; no system-specific username or password are used or maintained. Authorized users are controlled via FDA Active Directory groups. These assigned users can modify system content. For example, they may add new publications, manage/delete existing publication data, view order history, update the inventory, and view reports. The ePub Administrator System maintains the following non-PII data relative to each publication within the catalog: (a) publication title, (b) publication code, (c) publication description, (d) language, € downloadable, (f) hard copy availability, (g) maximum order quantity, and (h)available stock quantities.

The system also displays order history which includes the following non-PII data: (a) Order ID, (b), Order Date, (c) Order Details (includes publication title and publication code), (d) Order Quantity, and € Audience Type.

		The system displays the following PII data which is read-only for only authorized users: (a) First Name, (b) Last Name, (c), Business Street Address (d), Business Zip Code, (e) Business State, and (f) Contact Details (either Business Email or Business Phone Number). PII is stored per the HFP date records retention policy.
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.	Credentials are only used for the internal admin interface component. The external facing component does not require credentials.
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The information and PII about external users is collected and/or maintained in order to allow users to submit requests for hard copies of a publication and have that publication mailed to a specified address. This information is passed to the HHS Warehouse system who fulfills the shipping orders. The information about internal users is collected to establish catalog administrators for the system catalog. Only authorized FDA employees, DHHS employees, and direct contractors (internal users), who require access to perform their authorized duties can access this PII in the event that an order needs to be regenerated or a follow up with the requestor is required. EPub does not collect any other personal 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).	epublication.fda.gov epublication-admin.fda.gov
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 ePublication Online Ordering system (external component) can be accessed by navigating to the public URL. It provides the public with the ability to browse through FDA's Education Resource Library containing a catalog of printable educational materials and videos on topics related to food safety, nutrition (including labeling and dietary supplements), and cosmetics. Materials are available in PDF format for immediate download.
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No

PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Biographical Information Name Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	<100
PIA 25:	For what primary purpose is the PII used?	The FDA uses the PII for the primary purpose of fulfilling hard copy orders of publications to users who have requested it.
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.	There are no legal authorities that govern information use and disclosures specific to the system.
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 Email 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.	OMB information collection approval number is not required because information collection is voluntary.
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.	The PII is shared and disclosed with the HHS Program Support Center (PSC) Elite Series System (Elite System) so that their system can fulfil hard copy orders submitted through the EPUB system.

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)).	The following Interconnection Security Agreement between: Program Support Center (PSC) Elite Series System (Elite System) And U.S. Food and Drug Administration (FDA) Electronic Publications (E-Pub) agreement is in place.
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.	The system stores all order generation records and submissions via system logs and reporting mechanisms for system admins to track and monitor.
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.	N/A, voluntary submission
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.	When major changes occur to the system, the process in place to notify users is to put a banner on the landing page notifying users of the changes.
PIA 36:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	The processes in place to resolve an individual's concerns when they PII has been inappropriately obtained, used or disclosed include logging a ticket with the IT support help desk, reviewing access logs, and troubleshooting the incident to validate claims.
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.	HFP performs annual reviews to evaluate user access. One of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified during system use are addressed when discovered. 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. 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.
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.	Contractors serve as both Administrator and Developer, see reasons below: Developers require access to PII to provide appropriate maintenance and system debugging services for the system. Administrators require access to PII about users to track and follow up on order statuses with the HHS warehouse as users inquire about them.
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 by following the system Role Based Access Controls established for the system. Only authorized and approved users designated by the System Owner may be granted access.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	The following technical methods are in place to allow those with access to PII to only access the minimum amount of information necessary to perform the job: Role Based Access Controls and Privileges.
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 internal and system support users for EPUB are required to complete the FDA's annual privacy, cybersecurity awareness, and information protection training and awareness programs to make them aware of protecting PII.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	No additional system-specific training is received by users, however: (example: users are provided with user guides and manuals and privacy guidance is available on the FDA intranet and from Privacy staff).
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The following process and guidelines are in place for the retention and destruction of PII: The specific NARA records schedule is General Records Schedule (GRS) 6.5 File Code: 020 Consumer/client records: Distribution lists used by an agency to deliver specific goods or services. Records include contact information for customers or clients, subscription databases for distributing information such as publications and data sets produced by the agency, files and databases related to constituent and community outreach or relations, and sign-up, request, and opt-out forms. Disposition: DAA-GRS-2017-0002-0002 Temporary. Delete when superseded, obsolete, or when customer requests the agency to remove the records.

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.	FDA secures PII in the system using the following administrative controls: Role-Based Access Control (RBAC) and SSO. FDA secures PII in the system using the following technical controls: Amazon Web Services (AWS) GovCloud, Federal Information Security Modernization Act (FISMA) Moderate Classified Services.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	6/27/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/27/2025
SOP Review Comments:		**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/27/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 6/27/2025 All comments have been addressed. This PIA is ready for SAOP review and approval. 6/26/2025 Please see comments and update accordingly: PIA-38: Per PTA-5, Direct Contractors are internal users who have access to PII so "Contractor" should be selected. PIA-38A: Select "HHS/OpDiv Direct Contractors." PIA-38B" Select "Yes." PIA-39: Provide Contractor's reason to access PII. If contractors are both Administrator and Developers then you can say "Contractors serve as both Administrator and Developer." PIA-45: Please spell out RBAC, AWS, and FISMA.	**# of Days - APA Review:**	0

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/27/2025
SAOP Review Comments:	6/27/2025 Approved on behalf of the SAOP	**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/27/2025 12:58 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	6/23/2025	6/23/2025 FDA's Email (unable to attached email and PIA): The PIA is experiencing an Archer error with Question #3 of the general information (Q-3 “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. The ATO date is 5/29/2025. At this time, we are unable to update Archer to reflect the correct answer “Yes.”	
PIA 45	BLAND, CRYSTAL	6/26/2025	Please spell out RBAC, AWS, and FISMA.	
PIA 38	BLAND, CRYSTAL	6/26/2025	PIA-38: Per PTA-5, Direct Contractors are internal users who have access to PII so "Contractor" should be selected. PIA-38A: Select "HHS/OpDiv Direct Contractors." PIA-38B" Select "Yes."	
PIA 39	BLAND, CRYSTAL	6/26/2025	Provide Contractor's reason to access PII. If contractors are both Administrator and Developers then you can say "Contractors serve as both Administrator and Developer."	