PTA / PIA: FDA - SBNLE - QTR2 - 2025 - FDA4915794

Created Date: 4/9/2025 12:28 PM Last Updated: 4/15/2025 8:39 AM

General Information

PTA / PIA Name:	FDA - SBNLE - QTR2 - 2025 - FDA4915794	**PTA / PIA ID:**	2988831
Component Name:	FDA - HFP Small Business Nutrition Labeling Exemption	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	7
Submitter:		**Submit Date:**	4/9/2025
Next Assessment Date:	04/14/2028	**Expiration Date:**	4/14/2028
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.	12/23/2022
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	Carrol Burgundy
PTA 01A:	POC Title and Organization	HFP Privacy officer
PTA 01B:	POC Email Address	carrol.burgundy@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-2158
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 purpose(s) of the Human Foods Program (HFP) Small Business Nutrition Labeling Exemption System (SBNLE) is to meet the requirements of packaged foods and dietary supplements to bear nutrition labeling unless they qualify for an exemption. The relationship of HFP SBNLE to other FDA systems/components/information collections: this system was umbrellaed under CFSAN Foods Safety & Nutrition Submission Applications (CFSNSA). **However, the system was split individually amongst the apps covered under the boundary.** The key functional elements of the system include: The Federal Food, Drug, and Cosmetic Act requires packaged foods and dietary supplements to bear nutrition labeling unless they qualify for an exemption. The nutrition labeling exemptions for low-volume products found in 21 CFR 101.9(j)(18) and 21 CFR 101.36(h)(2) apply if the person claiming the exemption employs fewer than an average of 100 full-time equivalent employees and fewer than 100,000 units of that product is sold in the United States in a 12-month period. For these exemptions, a notice must be filed annually with FDA. The Small Business Nutrition Labeling Exemption (SBNLE) notice allows small businesses with low volume product production to be exempt from FDA's nutrition labeling requirements unless a health or nutrient claim is made. The exemption applies if the business employs fewer than 100 full-time equivalent employees, and fewer than 100,000 units of that product are sold in the United States in a 12-month period. SBNLE provides an online submission system for small businesses to notify FDA that they qualify for a nutrition labeling exemption. System "users" consist of: SBNLE includes two user modules. Users of the external module include retailers and owners of small businesses, who only require a user account (email address and password as well as token factor authentication) to access the system. Users of the internal module is limited to a very small group of FDA employees (permanent and Direct Contractors) serving in the role of administrators and developers.

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.	HFP Small Business Nutrition Labeling Exemption (SBNLE) collects and maintains the following personally identifiable information (PII) about FDA employees (permanent and Direct Contractors): (a) first and last name; (b) job title; (c) program. HFP SBNLE also collects PII about external users of the system, including firm contact names, mailing addresses, phone number and email addresses. The types of data that are maintained in and/or shared from the system is/are: The FDA system providing employee data is the Enterprise Administrative Support Environment (EASE) system (the subject of a separate assessment). Employee data is used to log on authorized users automatically and securely. SBNLE also retrieves information from other FDA systems, including the Field Accomplishments and Compliance Tracking System (FACTS) database to determine a company type (i.e., manufacturer or importer) based upon their Federal Employer Identification (FEI) number. Non-PII collected and maintained in the system includes regulatory compliance data, such as time period for the exemption, number of employees, products sold, and volume of product sold. The amount of time the PII is stored in the system is: SBNLE adheres to NARA approved GRS 5.2 Item 020 schedule for intermediary records. Therefore, PII records are reviewed during the periodic User Access Review process and retained or destroyed when no longer needed for business use.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	Active Directory

PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The SBNLE system contains information submitted by businesses seeking an exemption, including the firm type, name, mailing address, phone number, e-mail address, time period for the exemption, number of employees, volume of product sold, and the name, title, and phone number for the firm's contact person. SBNLE also retrieves information from other FDA systems, including the Field Accomplishments and Compliance Tracking System (FACTS) database to determine a company type (i.e., manufacturer or importer) based upon their Federal Employer Identification (FEI) number. SBNLE retrieves FDA employee data from the Enterprise Administrative Support Environment (EASE) system to automatically and securely log on authorized users. For FDA employees, the only identifying information collected via the SBNLE system is work contact information, as well as information about the User ID and the user's rights and roles within the system. FDA employees and Direct Contractors who access or use these applications do not use any PII to retrieve records held in the SBNLE application. The SBNLE system is Single Sign On (SSO) and PIV enabled for internal users. The system has implemented a multifactor authentication via alternate PIV cards for network access to privileged accounts. The FDA uniquely identifies and authenticates organizational users. For PIV authenticated system, PIV credentials are based on user's certification which are also unique. Users of the system include administrators and developers (FDA Direct Contractors). SBNLE utilizes PIV cards and Single Sign On (SSO). The authenticator is managed by Active Directory and all access is managed and granted through PIV/SSO. Users of the external module include retailers and owners of small businesses, who only require a user account (email address and password as well as token factor authentication) to access the system. PII from the system/component/collection about is shared with SBNLE shares PII with State or Local Agency/Agencies: Relevant information for industry points of contact may be supplied to state officials.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	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 Employment Status/History 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.	Job titles of industry points of contact, FDA employees. All information is work contact information.
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.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	The FDA uses the PII for the primary purpose of PII in SBNLE, includes Firm contact names, mailing addresses, phone and e-mail, is used to centrally track companies that have nutrition labeling exemptions. PII for FDA employees/direct contractors is used for SSO and PIV Card access.
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.	The legal authorities that govern information use and disclosures specific to the system and program are: Federal Information Processing Standards (FIPS) 199 NIST SP 800-60 Rev. 1, Volumes I and II. 15 U.S.C. 1453, 1454, 1455; 21 U.S.C. 321, 331, 342, 343, 348, 371; 42 U.S.C. 243, 264, 271.
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 Hard Copy Mail/Fax Online Government Sources Within the OPDIV Non-Government Sources Commercial Data Broker
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 Information Collection Approve Number: 0910-0381 Expiration Date: 9/30/2026
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.	State or Local Agency/Agencies
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 because: State or Local Agency/Agencies: Relevant information for industry points of contact may be supplied to state officials.
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)).	N/A
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 following process and procedures are in place for logging/tracking/accounting for the sharing and/or disclosing of PII: An accounting of disclosures would be made available if requested under Section (c) of the Privacy Act. All request for PII disclosure will be automatically sent to HFP Privacy and FOIA Team.
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.	When major changes occur to the system, the process in place to notify 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, or other available means to inform the individual. SNBLE system/program owners will contact HFP Privacy Team first if major changes were to occur.
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 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, or other available means to inform the individual. SNBLE system/program owners will contact HFP Privacy Team first if major changes were to occur.

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: Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have many avenues available for assistance. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC-employees or Direct Contractors only), 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 report without delay to FDA's Cybersecurity and Infrastructure Operations and Coordination Center (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.	The agency reviews PII during the approval and certification process. Availability, relevancy, accuracy, and integrity of PII about FDA employees is addressed at the source system, EASE, where reviews and controls are applied pursuant to security and privacy assessments of that system as well as under organizational business practices.
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: Receive, review, manage and track submissions. Administrators: Monitor the system, manage the workflow and control system access. Developers: For developing and testing new software releases and troubleshooting errors. Some of the developers are Direct Contractors. Contractors: Direct contractors who perform administrative, development, testing, and maintenance purpose.

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: Users who require access to the PII in the system need to obtain supervisory approval before access is granted. There are two ways to request access to the applications: the user emails the business owner/IT Technical Lead or submits a request online through the 'Request Access' application option.
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 security controls ensure that each user role is appropriately assigned at the individual level in accordance with an individual user's need-to-know and least-access-privileges in regard to official duties such that each user sees/accesses only that data that is essential to complete his/her job. The agency reviews the access list for the information system on a quarterly basis. During this process users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system.
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 personnel with access to PII collected in the SNBLE system are required to take mandatory FDA security and privacy awareness training annually.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	System/system component/information collection users also receive the following additional training: The SBNLE application has a user manual which serves as system reference material and training.
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).	SBNLE adheres to NARA approved GRS 5.2 Item 020 schedule for intermediary records. Therefore. PII records are reviewed during the periodic User Access Review process and retained or destroyed when no longer needed 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.	FDA secures PII in the system using the following administrative controls: Administrative safeguards include user training on PII and implementation of Need to Know and Minimum Necessary principles when awarding access. FDA secures PII in the system using the following technical controls: Technical Safeguards include the use of two-factor access authentication, device disk encryption, firewalls, virtual private network (VPN) and network monitoring and intrusion detection tools. FDA secures PII in the system using the following physical controls: Physical controls include the location of all system servers located at FDA 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:**	4/9/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	4/9/2025
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:**	4/15/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 4/15/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	6

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	4/15/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
4/15/2025 7:54 AM	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	4/11/2025	4/10/2025 Per FDA Email: • The Answer to PTA-5A is entered on the PTA but does not show on the PIA. ○ PTA-5A, Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is Active Directory. • 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 *11/21/2022*. • At this time, we are unable to update Archer to reflect the correct answer "Yes." The FDA Archer Team is aware of this occurrence and is working on a solution.	