Privacy Impact Assessment (PIA): FDA - Westat - QTR1 - 2025 - FDA4901213

Created Date: 2/13/2025 11:57 AM Last Updated: 3/5/2025 11:47 AM

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 - Westat - QTR1 - 2025 - FDA4901213	**PIA ID:**	2767106
Name of Component:	FDA - CDER Westat	**Name of ATO Boundary:**	CDER Westat
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	36
Submission Status:	Submitted	**Submit Date:**	1/28/2025
Next Assessment Date:	03/04/2028	**Expiration Date:**	3/4/2028
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4901213
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?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	8/13/2024
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?
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.
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.
PTA - 5A:	Are user credentials used to access the system?
PTA - 5B:	Please identify the type of user credentials used to access the system.
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.
PTA - 7:	Does the system collect, maintain, use or share PII?
PTA - 7A:	Does this include Sensitive PII as defined by HHS?
PTA - 8:	Does the system include a website or online application?
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?

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.	
PTA - 10:	Does the website have a posted privacy notice?	
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	
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?	
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?	
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?	
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?	
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	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 names and email addresses for the primary purposes of interview recruitment and scheduling. All other information collected relate to targeted interview questions about consumers' sunscreen-related purchase behavior and decision-making, which are taken from members of the general population of consumers, including an initial formative study sample (Phase I; N = 25) and larger follow-up study sample (Phase 2; N = 150).
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	There is 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 legal authority governing the FDA's authority to collect information about sunscreen-related purchases is 5 U.S.C. 301 and 21 USC 301. For the research, Westat and FDA also have Institutional Review Board (IRB) approval. Westat's IRB is formally known as the Westat Human Research Protections Program (HRPP) Office, and they reviewed and approved our study forms and materials on October 28, 2024 (FDA Sunscreen, Project Number 6781.12, Amendment Approval ID: 4275; FWA 00005551I). Our Westat IRB approval and all corresponding study materials are currently under FDA IRB review after they were submitted to the CDER Human Subject Protection Liaison.
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.	Directly from an individual about whom the information pertains In-person Online Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	The OMB Control Number is 0910-0697.
PIA - 10B:	Identify the OMB information collection approval number expiration date.	1/31/2027
PIA - 10C:	Explain why an OMB information collection approval number is not required.	
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.	Individuals may opt-out of the collection or use of their data/information at any time, without penalty, by letting our interviewer or project director know of their desire to have their PII removed from the study. They are also provided contact information should they have any questions or concerns after the study is completed.
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.	All participants participating in our research much complete an IRB- and OMB- approved consent form, which offers them the ability to participate on their own volition and withdraw their participation, at any time, without penalty.
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.	The processes in place to resolve an individual's concerns when their data/information has been inappropriately obtained, used, or disclosed, includes resolution either by contacting the Westat IRB and/or the Project Director. Contact information for both entities are provided in an FDA-approved Informed Consent Form. Individuals may also contact FDA with any concerns using information provided on FDA.gov.

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 process in place for periodic reviews of project information to ensure the data integrity is that the Contractor, Westat Inc., must have their system routinely checked for compliance by FDA's Office of Digital Transformation (ODT). In addition, Westat must remain in compliance concerning their PII and other ATO-related conditions throughout the enterprise performance life cycle (EPLC). Data accuracy is confirmed and ensured by the individual participants who provide their information directly to Westat. Data integrity is ensured by the implementation of security controls and compliance with the ATO process. Controls are selected based on 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. Data relevancy and availability are ensured by regular reviews. Data discrepancies identified in the course of system use are addressed when discovered.
PIA - 17:	Identify who will have access to the PII in the system.	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.	The reason the Contractors need access to study information is to carry out the contracted research, contact participants for study enrollment, and both analyze and report on key study findings to the FDA.
PIA - 19:	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 project information are using an encrypted system and password-protected access to study data to ensure that only the contractor and essential FDA project staff have access to the study data and findings. Access is granted based on permissions settings put in place by the administrator of the system. Users will only be granted permissions with the minimum necessary information to perform their work. Regular reviews are conducted to determine if permissions need to be altered or revoked.

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.	All data are saved on a password-protected system accessible only to assigned users at Westat. Unique system passwords are consistently updated on a 60-day basis. The FDA's Office of Digital Transformation (ODT) vetted this system to ensure system compliance and data integrity and confidentiality. Westat only provides permission to access PII to those who require the information to carry out their contractually obligated duties. Permissions are granted and revoked as needed to ensure minimum necessary use.
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.	All users for of the system are required to complete the mandatory FDA Computer Security Awareness Training (CSAT) annually. The FDA's Office of Digital Transformation (ODT) ensures compliance.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users must also complete IRB-required trainings on informed consent and research ethics.
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).	The CDER Westat records are maintained under the following National Archives and Records Administration (NARA) record: General Records Schedule (GRS) 3.2 items 30 and 31. The records disposition is temporary under disposition authority DAA-GRS2013-0006- 0004 and the records are deleted or destroyed 6 years after they are no longer needed or 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.	The Contractor, Westat, secures study information in their system using the following administrative, technical, and physical controls: 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 & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	1/28/2025
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:**	1/28/2025
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	3/5/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 3/5/2025 This PIA was SAOP approved outside of the Archer tool on 2/25/2025 (please see attached PIA in Supporting Documentation).	**Agency Privacy Analyst Days Open:**	36

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	3/5/2025 This PIA was SAOP approved outside of the Archer tool on 2/25/2025 (please see attached PIA in Supporting Documentation).	**SAOP Review Date:**	3/5/2025
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
2-11-2025 CDER Westat_SOP Approved_PA Approved.rtf	660346	.rtf	2/13/2025 12:05 PM	0
2-25-2025 CDER Westat_SAOP Approved.rtf	657767	.rtf	2/26/2025 7:55 AM	0
CDER Westat_SOP Approved_OpDiv Draft.pdf	159030	.pdf	2/13/2025 12:05 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	2/13/2025	PTA is blank.	

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:	3/5/2025 11:47 AM	**History Log:**	View History Log