Privacy Impact Assessment (PIA): FDA - CEARS - QTR4 - 2024 - FDA4564261

Created Date: 11/5/2024 3:23 PM Last Updated: 11/7/2024 11:51 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 - CEARS - QTR4 - 2024 - FDA4564261	**PIA ID:**	2404978
Name of Component:	FDA - CBER Error and Accident Reporting System	**Name of ATO Boundary:**	CBER Office of Regulatory Operations
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	2
Submission Status:	Submitted	**Submit Date:**	11/5/2024
Next Assessment Date:	N/A	**Expiration Date:**	11/7/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4564261
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.	11/22/2022
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.	Not Applicable (N/A) - This is the initial dedicated PTA/PIA for CBER Error and Accident Reporting System (CEARS). There have been no changes to CEARS since FDA previously assessed it in a PIA that covered multiple components within the same system boundary.
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 Center for Biologics Evaluation and Review (CBER) Error and Accident Reporting System (CEARS) is an application that is one of many components of the CBER Office of Regulatory Operations (ORO) system. Other technology, systems and components within ORO are assessed separately. The Food and Drug Administration (FDA) previously assessed CEARS in conjunction with other elements of ORO and is now conducting this assessment to supplement previous assessments and ensure transparency. CEARS is used by FDA personnel to search for Biological Product Deviation (BPD) report information (formerly error and accident reports) that have been submitted to CBER since October 1994. CEARS supports searching on several different parameters including date of receipt, FDA district, FDA establishment identifier, or BPD codes. The query results are confidential and should not be released to the public.
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.	CEARS displays information about BPD reports submitted by biologic product manufacturers. Access to CEARS is through single sign-on. Individuals making these reports via CEARS provide name, telephone, and e-mail for contact purposes only and no other PII is contained in the application.
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.	CEARS provides the ability for users to query for BPD report data stored in the Biologics Compliance Information System (BCIS) such as the establishment reporting deviations, deviating establishments, deviation descriptions, root causes, follow-up actions taken, the affected product and unit information, and product disposition information. Data in this system is used to retrieve information about biologics manufacturers and the ingredients and the suppliers/manufacturers of the ingredients/substances that these manufacturers use in manufacturing. One use is to aid review: FDA reviewers are given information about all ingredients used in manufacturing described in an application, and they can search and find those same ingredients in other products. An important use is when FDA/CBER learns that an ingredient from one supplier is adulterated or counterfeit, FDA/CBER can quickly determine how many CBER biological products and manufacturers are at potential risk due to the counterfeit ingredient. Additionally, if there is a natural disaster, fire, or regional threat such as nuclear reactor leak, the key vendors/manufacturers of ingredients in those areas can be identified more quickly and allow for quicker responses to avert potential product shortages or potential harm to the public.
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.	CEARS has an FDA CBER internal website that is used to display information about BPD reports submitted by biologic product manufacturers. Access to CEARS is through the internal website uniform resource locator (URL) and verify their identity through Single-Sign On (SSO) multi-factor authentication. Individuals making these reports via CEARS provide name, telephone, and e-mail for contact purposes only and no other PII is contained in the application. Only CBER fulltime employees (FTEs) with specific access and role are able to access the system. The categories of individuals who have access to the website are those responsible for data entry, reviewers, and administrators.
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 Phone numbers 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.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	CBER uses the PII in this application to record, monitor, and manage the biological product information and reports received from the biological product manufacturers and communicate with them when circumstances require.

PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Secondary use of PII includes integration testing and research for linking patient outcomes to adverse events.
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 these applications is authorized by 5 U.S.C. 301, Federal Food, Drug and Cosmetic Act, 21 USC 353, 356b, 360; and the Public Health Service Act, 42 USC 263a. In addition, the security and privacy measures of the applications 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.	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Online Non-Government Sources Members of the Public Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	0910-0458 Expiration Date 02/28/2026 0910-0338 Expiration Date 10/31/2026
PIA - 10B:	Identify the OMB information collection approval number expiration date.	2/28/2026
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.	External individuals submitting biologic product reports are not mandated to submit any PII. External individuals voluntarily submit PII of a point of contact name and telephone number. This information is used to contact people to clarify data regarding their submissions. This information is provided as a convenience to aid in communications and is voluntary. There is no method for employees to opt out of submitting their PII. While submission is voluntary, permanent employees, Direct Contractors, fellows and other personnel must provide their PII in order for the Agency to process administrative materials and securely administer access to Agency information and property. Failure to provide this information may result in being unable to complete duties as required in their role at FDA.
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.	If a major change in the collection and use or sharing of PII data for this application occurs, users will be notified via individual e-mail notification or in updated notice statements on submission forms and Federal Register publications. However, no such changes that would affect the rights or interests of the individuals are anticipated.
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.	FDA personnel may resolve such concerns by contacting the appropriate system administrator, FDA’s Employee Resources and Information Center (ERIC), FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC), the FDA Privacy Office, and other FDA offices using contact information provided on all FDA internet and intranet pages. Any changes to an individual's name or address would need to be updated using a Standard Form 50 or 52, which is the process used to make such changes used by all FDA employees, and the data would be updated in the separate human resources information system. External individuals may use any of a number of avenues to raise concerns, including contacting FDA offices through FDA.gov, phone, e-mail, and mail. The concern will be directed to the responsible FDA office or division for further review and response. All FDA personnel are required to rapidly report any suspected or actual breach of PII or security incident.

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.	Individuals who submit their PII do so voluntarily. 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. 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 during providing the system with an authorization to operate (ATO). Controls are selected based on 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. CBER 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.
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- Industry submitters have access to the PII for submissions they make. FDA users will have access to PII to review and manage the reports received from product manufacturers. Note that "FDA users" may include subject individuals, supervisors, or business function administrators. Administrators- Business administrators may have access to PII to conduct business functions. System administrators may have access to PII to support system administration activities. Developers- Developers may have access to PII to maintain the system and provide technical assistance to users. Contractors- Some developers and system administrators may be Direct Contractors and will have access under the same circumstances as developers.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users who maintain the applications need to have supervisor approval before access is granted. The user's supervisor will use an account creation form to specify the minimum application access that is required in order for the user to complete his/her job. The agency reviews the access list for the application on a quarterly basis to review and adjust users' access permissions, and to remove unnecessary accounts from 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/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.	All system users at FDA take annual mandatory computer 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 (including any special restrictions on data use and/or disclosure). The FDA Office of Information Management and Technology (OIMT) verifies that training has been successfully completed.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Help links are available within applications, and instructional materials are available on the FDA Intranet for all applications. All users are instructed on adhering to the HHS Rules of Behavior in the context of their work involving this system. For additional privacy guidance, personnel may contact the Agency's Privacy Office. Privacy program materials are provided to personnel on a central Intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA.
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).	All Adverse Event files are temporary, and destroyed according to the instructions cited in the following records schedules: FDA 5, Adverse Event/Experience and Product Defect Reports; 5.1, Adverse Event Reports Management Files; 5.2, Adverse Event Reports or Forms; 5.3, Adverse Event Reporting Systems; 5.3.2, AERS Database Records; 5.3.3, Extracts of the Adverse Event Data for Public Access: Output Records; 5.1 and 5.2. CBER Records Control Schedule (National Archives and Records Administration NARA Schedule No. N1-088-03-05) Items B-34, Post Marketing Products Safety Reviews and Adverse Event Summaries, and B-35, Post-Marketing Surveillance Lot Analysis Reports. Records are retired to the Washington National Records Center three years after the cutoff date and destroyed 20 years after the cutoff date.

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.	There are several controls in place for securing of PII within the systems. The administrative controls include system users completing an access request form and an access review/approval process. The technical controls include firewalls, virtual private networks (VPNs), encryption, and intrusion detection systems. The physical controls are comprised of guarded facilities, gated access to these facilities, security barriers, and locked doors.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	11/5/2024
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:**	11/5/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	11/7/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 11/7/2024 All comments have been addressed. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	This PIA is also 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 reflecting "No" as the answer when the correct answer is "Yes." The FDA Archer Team is aware of this occurrence and is working on a solution.	**SAOP Review Date:**	11/7/2024
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
(11-6-2024) EMAIL_Priority PIA in Queue (CBER Error and Accident Reporting System).pdf	379486	.pdf	11/6/2024 8:47 AM	2
CBER Error and Accident Reporting System_SOP Approved.pdf	167699	.pdf	11/6/2024 8:47 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	VILLAFUERTE, NESTOR	11/6/2024	Q3 states that the system does not have an ATO and the planned ATO date has passed, please check for accuracy.	
PIA - 1	BLAND, CRYSTAL	11/7/2024	11/6/2024 Per FDA's email: This PIA is also 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 reflecting “No” as the answer when the correct answer is “Yes.” The FDA Archer Team is aware of this occurrence and is working on a solution.	

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:	11/7/2024 11:51 AM	**History Log:**	View History Log