Privacy Impact Assessment (PIA): FDA - BER - QTR1 - 2025 - FDA4914039

Created Date: 2/25/2025 7:30 PM Last Updated: 2/26/2025 12:31 PM

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 - BER - QTR1 - 2025 - FDA4914039	**PIA ID:**	2809463
Name of Component:	FDA - CBER Blood Establishment Registration	**Name of ATO Boundary:**	CBER Office of Regulatory Operations
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	1
Submission Status:	Submitted	**Submit Date:**	2/25/2025
Next Assessment Date:	N/A	**Expiration Date:**	2/26/2028
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4914039
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.	11/21/2022
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.	The Food and Drug Administration (FDA) has made no changes to this component since the last Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA) was approved.
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 Food and Drug Administration's (FDA) Center for Biologics Evaluation and Review (CBER) Office of Regulatory Operations (ORO) mission is to protect and enhance the public health through the regulation of biological and related products to include those that manufacture blood products. CBER ORO utilizes multiple applications to support this mission, including the subject of this assessment, the CBER Blood Establishment Registration (BER) system. CBER BER collects basic information about the blood product industry in order to meet its mission to conduct regulatory activities and assist in preventing the spread of disease. The baseline information collected enables FDA to efficiently and effectively respond to emerging public health concerns related to the manufacture of blood products, and in conducting inspections of related facilities. The list of industry members and their blood products assist the agency to disseminate educational materials and other important information regarding FDA policies and requirements. CBER BER is used to manage the submission, receipt, review, and maintenance of Blood Establishment Registrations (form FDA 2830). The system receives registration information from the CBER electronic Blood Establishment Information (eBER) system (the subject of a separate assessment), a web application used by industry (also known as Reporting Officials and US Agents) to electronically submit blood establishment registration information. BER also includes two query modules which can be used to view data contained in the system. eBER Intranet Query is used by certain authorized internal users (FDA permanent employees and Direct Contractors) at FDA Centers (Center for Biologic Evaluation and Research (CBER), Center for Devices and Radiological Health (CDRH), and the Office of Regulatory Affairs (ORA)) to view blood establishment registration information for active, inactive, and pre-registered firms collected by eBER and maintained in BER. eBER Internet Query is used by industry to view data collected and maintained in BER. Neither query module collects, maintains, or shares information. It is a view only tool that allows users to view blood establishment registration information for active, inactive and pre-registered firms.

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.	CBER BER maintains personally identifiable information (PII) about external individuals. As shared by eBER, PII maintained is contact information and consists of name, business email address, business phone number, and business mailing address. Information maintained in BER is viewable by internal FDA users via the eBER Intranet Query module. Non-PII maintained in the BER includes blood establishment registration information which includes Establishment Name, Establishment Function, Product listings, Establishment Status, State, Zip Code, and Country. Data elements collected for blood establishment registration are detailed on Form FDA-2830. For all of these applications, Reporting Officials and US Agents must provide a business telephone number and a business e-mail address. BER and eBER Intranet Query are used by authorized FDA network users and access to this system is granted via the CBER Menu application (the subject of a separate assessment) using single sign-on (SSO) authentication. Users of the system are FDA permanent employees and Direct Contractors with FDA badges and smart cards. Direct Contractors who maintain the system have access only for testing, deployment verification, and to provide user support. eBER industry users access the system through the CBER Online login portal. A username (work email address) and password are required. All data collected in the CBER ORO System is provided to users "as-is" in that it shares information that it has received from other source systems but does not create or modify any data it contains. Information about the users themselves (the medical reviewers, systems administrators) are managed through network access protocols and all have FDA system access credentials.
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.	BER maintains blood establishment registration information such as establishment name, name, business email address, business phone number, and business mailing address, and product information. This information provides the FDA with a list of establishments and products to inspect and to efficiently and effectively respond to emerging public health concerns. The establishment registration information is shared with FDA field inspectors.
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.	CBER BER provides access to quality information and improved efficiency in performing regulatory-mandated registration of blood establishments. BER is used to manage the submission, receipt, review, and maintenance of Blood Establishment Registrations (form FDA 2830). The system uses a web application component to allow facilities to submit registrations over the internet.
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 Mailing Address
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?	The PII collected by these systems is part of the required information to satisfy the regulatory requirement to register the cell/tissue or blood establishment or update the registration on an annual basis. The PII is contact information associated with the registration.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	A potential secondary use is integration testing.
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.	FDA regulates under the authority of section 361 of the Public Health Service (PHS) Act. Under section 361 of the PHS Act, FDA makes and enforces regulations necessary to prevent the introduction, transmission, or spread of communicable diseases. HCT/Ps that meet the criteria in 21 CFR part 1271 are regulated solely under section 361 of the PHS Act. HCT/Ps that do not meet all the criteria in part 1271 for regulation solely under section 361, are regulated as drugs, devices, and/or biological products under section 351 of the PHS Act and/or Food, Drug and Cosmetic Act. The implementation of these applications is also authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures of the applications are required by the Federal Information Security Management Act (FISMA) and the statutes underlying Office of Management and Budget (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 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.	eBER: FDA Form 2830. OMB No. 0910-0052
PIA - 10B:	Identify the OMB information collection approval number expiration date.	6/30/2026
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.	The reporting official is the person appointed by the owner or operator to register the form and answer all the correspondence and inquiries relative thereto. The United States Agent is a person residing or maintaining a place of business in the United States whom a foreign establishment designates as its agent. Reporting is required, but any person can serve as the industry member's Reporting Official or United States Agent, and reporting is not "mandatory" as that term is used by the Privacy Act. Individuals are not allowed to opt-out of the collection of name and address. This information is specified in the regulation. This information is used to contact people to clarify data associated with their registration.
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 email 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 who suspect their PII maintained by or on behalf of the FDA has been inappropriately obtained, used or disclosed have several avenues available to resolve the situation. Employees can work with their supervisors, the FDA Privacy Office, the Employee Resource and Information Center (ERIC), FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC), and other channels. Contact information for these offices and resources are available across FDA's internet and intranet pages. External individuals who suspect their PII maintained by or on behalf of the FDA has been inappropriately obtained, used or disclosed have several avenues available to resolve the situation. These individuals may contact the office or division where they have determined that their information is held. They may contact the FDA Privacy Office via email address provided on FDA.gov. FDA personnel are required to rapidly report any suspected or confirmed incidents or breaches to the FDA CIOCC. Contractors are required to safeguard all information and to report potential data breaches to the FDA.
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.	Submitter's PII is provided voluntarily by the individual. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. 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 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 registrations 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.	Before granting access, supervisors determine the minimum application access that is required in order for the user to complete 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 Digital Transformation (ODT) verifies that training has been successfully completed and maintains a record of certificates of training on all FDA employees and Direct Contractors.

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 Department of Health and Human Services (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).	DAA-GRS-2013-0001-0004-Temporary-Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
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 the securing of PII within the system. 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. 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:**	2/25/2025
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:**	2/25/2025
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/26/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 2/26/2025 No comments, FDA requested expediated processing relating to GAO matter. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	2/26/2025
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
2-24-2025 EMAIL_Priority PIA in Queue (CBER Human Cell and Tissue Establishment Registration System).pdf	403241	.pdf	2/26/2025 7:14 AM	0
2-25-2025 EMAIL_FW_ FDA Priority PIA Submissions.pdf	269363	.pdf	2/26/2025 7:57 AM	0
CBER Human Cell and Tissue Establishment Registration System_SOP Approved.pdf	173916	.pdf	2/26/2025 7:14 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	2/26/2025	Archer issue impacting the 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 *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.	

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:	2/26/2025 12:31 PM	**History Log:**	View History Log