Privacy Impact Assessment (PIA): FDA - HCTERS - QTR2 - 2021 - FDA1955831

Date Signed: 12/1/2021

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

Status:	Approved	**PIA ID:**	1329379
PIA Name:	FDA - HCTERS - QTR2 - 2021 - FDA1955831	**Title:**	FDA - CBER Office of Regulatory Operations
OpDIV:	FDA		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	No
PTA - 2:	Does the system include a website or online application?	No
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
PTA - 5A:	If yes, Date of Authorization	6/19/2018
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	No changes were made to the system. Updates to the dates for the following were made in this document: ATO date OMB information collection approval expiration dates
PTA - 8:	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?	FDA uses a set of information technology applications to collect registration information about regulated establishments and their

products. This assessment addresses multiple registration-supporting applications that are components of the Center for Biologics Evaluation and Review (CBER) Regulatory Management system.

FDA collects basic information about the Human Cell and Tissue Product (HCT/P) industry and its products in order to meet its mission to conduct regulatory activities and assist in preventing the spread of disease. The baseline information collected enables FDA efficiently and effectively to respond to emerging public health concerns related to human cells or tissues, and in conducting inspections. The list of industry members and their HCT/Ps assist the agency to disseminate educational materials and other important information regarding FDA policies and requirements.

Establishments must register and submit a list of every HCT/P that they manufacture. Registration with FDA is not indicative of an establishment's compliance with all applicable rules or regulations. The registration information does not include proprietary product information. The establishment information and the HCT/P listing is available to the public.

The electronic Human Cell and Tissue Establishment Registration System (eHCTERS) and electronic Blood Establishment Registration (eBER) systems allow industry users (also known as Reporting Officials and US Agents) to electronically submit and update establishment registration information over the Internet through a secure web server.

These systems allow authorized FDA users to create, update, administer, track and report on establishment registration and product listing information. The eHCTERS and eBER systems also include a query module that allows industry users to search on establishment registration information for active, inactive, and pre-registered firms.

The Human Cell and Tissue Establishment Registration System (HCTERS) internal system receives electronic Human Cell and Tissue Product (HCT/P) establishment registration submissions from the Electronic Human Cell and Tissue Establishment Registration System (eHCTERS) external system, and allows authorized FDA users to create, update, administer, track and report on HCT/P establishment registration and product listing information. In addition, an eHCTERS Intranet Query is available to certain authorized FDA employee users at some FDA Centers (Center for Biologic Evaluation and Research (CBER), Center for Devices and Radiological Health (CDRH), and the Office of Regulatory Affairs (ORA)) within the FDA firewall to search for HCT/P establishment registration information for active, inactive and pre-registered firms.

PTA - 9:	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.	eHCTERS collects cell and tissue establishment registration information. It shares that information with eHCTERS and is viewable by FDA users via the eHCTERS Intranet Query. eBER collects blood establishment registration information. It shares that information with BER and is viewable by internal FDA users via the eBER Intranet Query. eBER, eHCTERS, and BER collect and contain PII for external individuals. For HCTERS. PII is mainly about external individuals except for one screen that allows for the maintenance of a list of FDA District Contacts for Tissue Establishment Registration. The Intranet Query tools do not contain information; they are search tools used in conjunction with the other applications. Data elements collected for blood and tissue establishment registration are detailed on Form FDA-3356 for Tissue and Form FDA-2830 for Blood. For all of these applications, Reporting Officials and US Agents must provide a business telephone number and a business e-mail address. eBER and eHCTERS industry users access the systems through the CBER Online login portal. A username and password are required. BER, HCTERS, and both Intranet Query tools are used by FDA users only, and access is role-based single sign on. Direct contractors who maintain the system have access only for testing, deployment verification, and to provide user support.
PTA - 10:	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	These systems collect cell and tissue establishment registration information such as establishment name, point of contact, contact information, and a list of HCT/Ps that the establishments recover, process, package, store, label, distribute, and screen or test. Screening or testing may involve testing the HCT/P donor individual. 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. BER maintains blood establishment registration information such as establishment name, point of contact, contact information, 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 - 10A:	Are records in the system retrieved by one or more PII data elements?	No

PTA - 11:	Does the system collect, maintain, use or share PII?	Yes
	PIA	
PIA - 1:	Indicate the type of PII that the system will collect or maintain	Name E-Mail Address Phone numbers Mailing Address
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Public Citizens Other
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 - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	FDA regulates HCT/Ps 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 - 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 - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	eHCTERS: FDA Form 3356. OMB No. 0910-0543. Expires 07/31/2023.

		eBER: FDA Form 2830. OMB No. 0910-0052. Expires 06/30/2021.
PIA - 9B:	Identify the OMB information collection expiration date.	7/31/2023
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	The HCT/P and Blood registration information is collected directly from individuals using FDA form 3356 (HCT/P) or form 2830 (Blood) which includes information about the applicable regulations and instructions. Methods of notification include Federal Register publications, this assessment, privacy statements on FDA.gov and other resources provided on FDA.gov such as system user instructions. Methods of notification for FDA users include Federal Register publications, privacy statements on FDA.gov, this assessment, and other resources provided on FDA.gov such as system user instructions. FDA personnel (employees, direct contractors, fellows, etc.) are notified at the time of hire and consent to the submission and use of their personal information as a condition of employment. FDA center representatives, and the various individuals involved with the specific data collection and use provide notification to the employees and non-employees at the time the data is requested.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	Describe the method for individuals to 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 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	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. Internal users have all these avenues available as well as a 24x7 technical assistance hotline, system administrators, supervisors, and more.
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 authority to operate (ATO). 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. 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 and the reason why they require access	Users Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17 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 - 17B:	Select the type of contractor	HHS/OpDiv Direct Contractor
PIA - 18:	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 - 19:	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 - 20:	Identify training and awareness provided to personnel (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 and maintains a record of certificates of training on all FDA employees and direct contractors.
PIA - 21:	Describe 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 NARA records retention schedule(s) and include the retention period(s)	Establishment registrations are retained as long as they are needed for business use, following disposition authority DAA-GRS 2013-00010004.
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.