Privacy Impact Assessment (PIA): FDA - IRB SST - QTR1 - 2024 - FDA2127395

Created Date: 3/20/2024 12:08 PM Last Updated: 4/29/2024 2:08 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 - IRB SST - QTR1 - 2024 - FDA2127395	**PIA ID:**	1785581
Name of Component:	FDA - CDER Institutional Review Board Site Selection Tool	**Name of ATO Boundary:**	CBER Office of Regulatory Operations
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	41
Submission Status:	Submitted	**Submit Date:**	4/18/2024
Next Assessment Date:	N/A	**Expiration Date:**	4/29/2027
Office:		**OPDIV:**	FDA
Security Categorization:	Moderate	**OpDiv PIA ID:**	FDA2127395
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)?	Yes
4:	ATO Date or Planned ATO Date.	10/12/2023
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.	Since this Privacy Threshold Analysis/Privacy Impact Assessment was last approved, FDA made the following changes to the [system/component/information collection] New Structured Query Language (SQL) Servers and New Windows Servers were installed by Office of Information Management and Technology (OIMT) due to EOL servers. Data Refreshes and minor functionality enhancements have been made.
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 FDA is responsible for conducting Institutional Review Board (IRB) inspections of IRBs (IRB) that oversee clinical and nonclinical research trials (IRB Site Selection Tool provides the means to identify IRBs to inspect). FDA's Center for Drug Evaluation and Research (CDER) established the Office of Bioresearch Monitoring (BIMO) to ensure the quality and integrity of data submitted to the agency in support of new product approvals and marketing applications, as well as to provide for protection of the rights and welfare of the thousands of human and animal subjects involved in FDA-regulated research. The program is implemented domestically and internationally through compliance programs resulting in over 1500 inspections annually.] The IRB Site Selection Tool receives information related to the various IRB entities from the National Institutes of Health (NIH) Office for Human Research Protections (OHRP) Database. PII data is collected which only professional contact information only. Fat files are retrieved from NIH (email, file share, etc.) and then an FDA employee loads the data set in a common secure repository that is utilized by IRB Site Selection Tool staff members. The sharing of data within the FDA is similar in nature. The same retrieval of information exists with FDA's Field Accomplishments and Compliance Tracking System (FACTS)/Complis, and FDA's Biomedical Research Medical Information System (BrMIS). This systems/applications are covered under separate Privacy Impact Assessments (PIAs). Additionally, in order to perform inspections, CDER IRB Site Selection Tool personnel (FDA employees and/or Direct Contractors) generate a file that the FDA personnel (Employees and/or Direct Contractors) send to CDER (Center for Drug Evaluation and Research) BIMO (Bioresearch Monitoring) Information Tracking Environment (CBITE) which is ingested by the system. The only PII data shared with CBITE consists of the IRB points-of-contact (POCs) work contact information only. Users of the system are: Administrators, Super User (multiple Center access), Reviewers (specific center access) Users of the system consists of reviewer, super users and Administrators. All of the users are FDA employees and Direct Contractors. All users access the system using Single sign-on (SSO)/Personal Identity Verification (PIV) credentials.

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.	IRB Site Selection Tool collects the following PII to identify POC for IRB inspections: first name and last name, professional email address, professional phone number, professional mailing address, and job title. The PII data is stored indefinitely or until user group indicates that there is no use for the data. IRB SST collects the following non-PII information not related to the POC but to the IRB entity: Registry data, Inspections, Applications. The system is utilized by FDA Centers: CDER, CBER (Center for Biologics Evaluation and Research), and CDRH (Center for Devices and Radiological Health) – users from the different centers see IRB entities from their center unless they are a Super User who has access to all Centers. Each center has access to the same type of information but filtered for their center.
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 Username
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.	IRB Site Selection Tool (SST) collects the following PII to identify POC for IRB inspections: first name and last name, professional email address, professional phone number, professional mailing address, and job title. The IRB Site Selection Tool is used to assess risk exclusively to the rights and welfare of humans participating as subjects in research, select IRBs for inspection, assign specific IRB inspections to reviewers, and to allow the Office of Bioresearch Monitoring to research information about IRBs.
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.	The primary purpose of the PII data in the IRB Site Selection Tool (SST) is to identify the IRB POCs, to discuss IRB inspections and to contact the relevant POCs, if necessary.
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 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?	The primary purpose of the PII data in the IRB SST is to identify the IRB POCs to discuss IRB inspections and to contact the relevant POCs, if necessary.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Not Applicable

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 authorities that govern information use and disclosures specific to the system and program are…. Food Drug, and Cosmetic Act (21 U.S.C. 301); 45 CFR Part 46 Subpart A.
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 Email Online Government Sources Within the OPDIV Other HHS OPDIV
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	OMB Control No: 0910-0130
PIA - 10B:	Identify the OMB information collection approval number expiration date.	12/31/2026
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Within HHS

PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	IRB does not collect data about its end-users. IRB SST is utilized by CDRH and CBER for IRB inspection identification. This is only on POC professional information to send to CDER BIMO Information Tracking Environment (CBITE) for setting up inspections. PII data collected for IRB is obtained from other systems (FDA's FACTS/Complis, FDA's Bioresearch Monitoring Information System (BrMIS), and the NIH OHRP Database and HHS IRB Registry). Notice to individuals would be provided in the context of the source systems. For the FDA source systems, FDA maintains separate Privacy Impact Assessments (PIAs) describing the notice provided to individuals. The National Institutes of Health (NIH) is responsible for maintaining appropriate privacy laws, policies, regulations including providing notice to individuals when collecting PII for the OHRP Database. At the time of hire and subsequently, FDA personnel and Direct Contractors are provided notice of the agency's expected creation and use of PII about them for purposes of authorized agency activities.
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)).	The following MOU agreement is in place, Human Assurance Tracking System (HATS)-FDA- The other NIH or Agency System Information, for FDA's Institutional Review Board Site Selection Tool (IRB Site Selection Tool) and NIH for receiving and storing OHRP IRB Registration data.
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.	Internal audit tables log and track changes to the data and when data is downloaded for CBITE processing. User logs are reviewed weekly and provided to security as part of annual security auditing of system under SDRT program.
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 IRB Site Selection Tool obtains PII about IRB POC from several different sources (FDA, HHS and NIH systems). Individuals for whom PII data is collected are made fully aware (when collected from the originating system) that PII data is required for reviewers to identify POCs for inspections. It is the responsibility of the originating system collecting the PII data to notify individuals of PII collection and providing an opt-out option.

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.	No major changes are planned or anticipated. However, should any changes occur, FDA would use the email addresses provided by the individual in the system to notify the user base of any proposed changes.
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.	Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any have multiple options available to resolve the issue. These individuals may contact FDA via email, phone and standard mail avenues (all of the relevant contact information is listed on fda.gov). They may also contact the FDA's Privacy Office or the Systems Management Center (SMC). Additionally, internal individuals may raise concerns through supervisory channels and through the FDA's Employee Resource and Information Center (ERIC). In the event of a security incident or breach of PII, the IRB Site Selection Tool system owner (SO) immediately contacts the FDA Systems Management Center, contracting officer representative (COR), contracting officer (CO), and the FDA Senior Official for Privacy.
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 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 in the course of providing the system with an authority 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. System administrators perform annual reviews to evaluate user access.
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 - Exclusively FDA employees who work with the IRB data to select IRBs for inspections and assign reviewers to IRBs. Administrators - Administrators have management roles and functions for administrative and auditing purposes. Some administrators are Direct Contractors. Developers - Developers are Direct Contractors for development purposes. Contractors - Some of the Administrators and Developers of the IRB Site Selection Tools are Direct Contractors.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The System Owner (SO) receives an email request to add a new user. Upon receiving the request, the SO sends an email to the administrator with instructions for adding the new user with the appropriate role-based access control (RBAC) and indicating the FDA center. The administrator creates the new user account following the instructions of RBAC by assigning the level of access based on the new user's role and function. The IRB Site Selection Tool user account permission levels are: (a) Disabled; (b) Super User; (c) CDER Review – End User; (d) CBER Review – End-User; (e) CDRH Review – End-User and (f) Administrator.
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.	The IRB Site Selection Tool uses role-based security, determined by the business needs of the user, to ensure minimum necessary access. The IRB Site Selection Tool has three roles, which cannot be combined. End-User/Reviewers have access to IRB data associated with their respective FDA Center. Super-Users have view access to all IRB data regardless of FDA Center. Administrators have view access to all IRB data regardless of FDA Center, update registry data, manage IRB Site Selection Tool accounts, and review access logs. All users are authenticated by FDA enterprise-wide Single Sign-On. Once a user is successfully authenticated by FDA SSO, the IRB Site Selection Tool provides access based on user role, controlling access to data and system functionalities.
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).	Users receive demonstrations and a thorough users guide describing how to work with the IRB Site Selection Tool.
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).	PII in the IRB Site Selection Tool is covered under General Records Schedule 3.2 “Information Security Systems Records”, Item 31 “systems requiring special accountability for access.” The disposition instruction is to destroy 6 years after password is altered or user account terminated but longer retention is authorized if required for business needs.” The disposition authority is under DAA-GRS-2013-0006-0004.
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 IRB Site Selection Tool is protected by physical, administrative, and technical controls at the system level and at the agency level in accordance with policies and regulations form the FDA, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB). Physical controls include secure access-controlled FDA property and PIV-cards. Users accessing the IRB Site Selection Tool remotely must follow FDA guidelines for physically securing hardware and using virtual private network (VPN). Administrative controls include security procedures, policies and access privilege management. The IRB Site Selection Tool logs all activities; IRB Site Selection Tool Administrator performs periodic reviews of the audit logs and acts on findings accordingly. The appropriate FDA personnel audit the system’s operating system (OS) logs. Technical controls include firewall, passwords, VPN, encryption and intrusion detection. The IRB Site Selection Tool resides on the FDA intranet inside the firewall with no communication to external systems. The IRB Site Selection Tool can only be accessed by users authenticated by the FDA Active Directory (AD) on the FDA network, using single sign-on. Security procedures are reviewed on a periodic basis to ensure that they are implemented correctly, operating as intended, and producing the desired results of protecting all information within the system.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	4/18/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	4/18/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	4/23/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 4/23/2024 All comments have been address, this PIA is ready for SAOP review and approval. 3/25/2024 A majority of the acronyms that were not spelled out in the PTA have been spelled out in the PIA. There are a few acronyms in the PIA that still need to be spelled out on first use.	**Agency Privacy Analyst Days Open:**	5

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	4/29/2024
		SAOP Days Open:	6

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
CDER Institutional Review Board Site Selection Tool_SOP Approved.pdf	184719	.pdf	3/21/2024 8:01 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	3/25/2024	Updates for the next iteration of the PTA: PTA-5: Please spell out acronyms SQL, OIMT, FACTS, CBITE, and SSO/PIV on first use.	
PIA - 11B	BLAND, CRYSTAL	3/25/2024	Please spell out "BrMIS" on first use.	
PIA - 11C	BLAND, CRYSTAL	3/25/2024	Please spell out HATS on first use.	
PIA - 16	BLAND, CRYSTAL	3/25/2024	Please spell out NIST on first use.	

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:	4/29/2024 2:08 PM	**History Log:**	View History Log