PTA / PIA: FDA - BEST - QTR3 - 2025 - FDA4950128

Created Date: 8/12/2025 4:43 PM Last Updated: 8/29/2025 4:42 PM

## General Information

| | | | |
|---|---|---|---|
| **PTA / PIA Name:** | FDA - BEST - QTR3 - 2025 - FDA4950128 | **PTA / PIA ID:** | 3640116 |
| **Component Name:** | FDA - CBER Biologics Effectiveness and Safety Innovative Methods | **ATO Boundary Name:** | CBER Hive |
| **Overall Status:** | Complete | **# of Days - Open:** | 17 |
| **Submitter:** | | **Submit Date:** | 8/12/2025 |
| **Next Assessment Date:** | 08/28/2028 | **Expiration Date:** | 8/28/2028 |
| **Office:** | | **OpDiv:** | FDA |
| **Security Categorization:** | High | | |
| **Make PIA available to Public?:** | Yes | **PIA Required:** | Yes |

| | | |
|---|---|---|
| **General 01:** | Identify the Enterprise Performance Lifecycle Phase of the system. | Initiation |
| **General 02:** | Is this a FISMA-Reportable system? | No |
| **General 03:** | Does the system have or is it covered by a Security Authorization to Operate (ATO)? | No |
| **General 04:** | ATO Date or Planned ATO Date. | 12/31/2025 |
| **General 05:** | Is the system or electronic information collection, agency or contractor operated? | Agency |
| **History Log:** | View History Log | |

## Privacy Threshold Analysis

### Privacy Threshold Analysis

| | | |
|---|---|---|
| **PTA 01:** | Point of Contact (POC) Name | Hussein Ezzeldin |
| **PTA 01A:** | POC Title and Organization | POC Title: BEST FHIR Program Manager<br>POC Organization: CBER/OBPV/DABRA |
| **PTA 01B:** | POC Email Address | Hussein.Ezzeldin@fda.hhs.gov |
| **PTA 01C:** | POC Phone Number | 240-402-8629 |
| **PTA 02:** | Indicate the following reason(s) for this PTA. Choose from the following options. | New |
| **PTA 03:** | Is the data contained in the system owned by the agency or contractor? | Agency |

| | | |
|---|---|---|
| **PTA 04:** | Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS. | The purpose of the Post market Safety and Surveillance (PS&S) Center for Biologics Evaluation and Research (CBER) Biologics Effectiveness and Safety (BEST) Platform is to deploy the BEST Platform, which is comprised of a data quality service, a Chart Review Application, a Case Management tool, and a detection and reporting services. The BEST Platform will be used within the Food and Drug Administration (FDA) as a system to receive and review case data transmitted from the eHealth Exchange Network. This Platform will allow CBER BEST authorized users to utilize the feasibility of the (FHIR) platform, as well as support gathering and evaluating technical and security requirements necessary for eventual development into a case review system for FDA.<br><br>The interface between the BEST Platform and other FDA systems/components/information collections is minimal. It will not directly interface with any CBER systems beyond what is necessary for user validation and information sharing between the BEST Platform and the eHealth Exchange.<br><br>The key functional elements of the system include the ability to retrieve and store electronic health records (EHR) data obtained from the eHealth Exchange to be viewed by authorized FDA users when identifying potential adverse event cases.<br><br>System “users” consist of CBER Subject Matter Experts (SMEs) and BEST Direct contractors serving in various roles to review data or manage the BEST Platform. |

| | | |
|---|---|---|
| **PTA 05:** | List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored. | The information collected under the PS & S CBER Biologics Effectiveness and Safety (BEST) Platform will consist of complete EHR clinical data such as medical records, medical record number, patient Id number, demographics, medications, conditions, immunizations, allergies, and diagnoses. In addition to EHR clinical data, the BEST Platform will collect the following personally identifiable information (PII) about patients: Name, Date of Birth, Mailing Address, email address, and phone number to populate potential adverse event reports. The BEST Platform will also collect information about the individual involved in the healthcare encounter, other than the patient, for example the Practitioner providing service, along with the Practitioner's qualification, such certification, licenses, or training pertaining to the provision of care.<br>The system will ingest and store data within the Postgres and MongoDB databases that are deployed on the CBER's High-performance Integrated Virtual Environment (HIVE), within specific controlled data containers only. Approved, verified users will view data via an authenticated login to a web-based application and will not be able to retrieve or store any data outside the application.<br>PII will be stored in the system he EHR clinical data will be deidentified for safety monitoring and evaluation activities. |
| **PTA 05A:** | Are user credentials used to access the system? | Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. |
| **PTA 05C:** | Please identify the system that maintains the user credentials or controls access to this system. | Active Directory |
| **PTA 06:** | Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual. | The PS & S CBER Biologics Effectiveness and Safety (BEST) Platform will retrieve and store EHR data originally pulled into the CBER's HIVE via the eHealth Exchange network connection to participant healthcare providers' FHIR endpoints. The eHealth Exchange acts as a hub through which health data can be exchanged. This exchange platform will request, retrieve, and store data on CBER's HIVE which will then be pulled to the FDA on-premises system described in this document. This will enable FDA users to view electronic health exchange information related to potential adverse reaction reports. This information is maintained in the CBER's HIVE and then loaded to the BEST Platform at FDA to evaluate the FHIR data and to allow CBER SMEs to review data contents for requirements gathering and fitness of system resolution/granularity.<br>The PII that is stored, received, accessed, or viewed as part of the BEST Platform is necessary for a comprehensive evaluation of the FHIR data exchange; without it the evaluation would be ineffective and insufficient.<br>CBER does not expect or plan to share data with another system. |

| | | |
|---|---|---|
| **PTA 07:** | Does the system collect, maintain, use, or share PII? | Yes |
| **PTA 08:** | Does the system include a website or online application? | Yes |
| **PTA 08A:** | Provide the URL(s). | https://bestim.fda.gov<br>https://bestim-dev.fda.gov/<br>https://bestim-qa.fda.gov/ |
| **PTA 08B:** | Are any of the website or online applications accessible by the public (including publicly accessible log in pages)? | No |
| **PTA 09:** | 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 purpose of the website is to provide CBER Subject Matter Experts (SMEs) with a tool that will allow users to review potential adverse event cases. Only those FDA employees identified as needing access to perform their authorized duties will be provided credentials and a log in capability. All users must authenticate their identity and log in to their account to access any data.<br><br>The following categories of individuals have access to the website: CBER SMEs.<br><br>Users access the website via an FDA controlled URL and login. |
| **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 12:** | Does the website use web measurement and customization technology? | Yes |
| **PTA 12A:** | Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII. | Session Cookies- Does Not Collect PII |
| **PTA 13:** | Does the website have any information or pages directed at children under the age of thirteen? | No |
| **PTA 14:** | Does the system have a mobile application? | No |
| **PTA 20:** | Are any third-party websites or applications (TPWA) associated with the system? | No |
| **PTA 21:** | Does this system use artificial intelligence (AI) tools or technologies? | No |

## Privacy Impact Assessment

### Privacy Impact Assessment

| | | |
|---|---|---|
| **PIA 22:** | Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share. | Biographical Information<br>Name<br>Date of Birth<br>Contact Information<br>Email Address (Personal)<br>Mailing Address (Personal)<br>Phone Numbers (Personal)<br>Email Address (Business)<br>Mailing Address (Business)<br>Phone Numbers (Business)<br>Medical Information<br>Medical Records<br>Medical Records Number<br>Patient ID Number |
| **PIA 23:** | Indicate the categories of individuals about whom PII is collected, maintained, or shared. | Patients<br>Members of the public |
| **PIA 24:** | Indicate the approximate number of individuals whose PII is maintained in the system. | 500 – 4,999 |
| **PIA 25:** | For what primary purpose is the PII used? | The FDA uses the collected PII in the course of reviewing potential adverse event cases resulting from the use of a biologic product. Data received into the PS & S CBER Biologics Effectiveness and Safety (BEST) Platform will include information about any population that is able to receive a vaccination (e.g., adults, minors). |
| **PIA 26:** | Describe any secondary uses for which the PII will be used (e.g., testing, training, or research). | BEST PII is not used in other contexts or for purposes unrelated to biologic product safety oversight. FDA does not use BEST PII in the course of information/IT system testing (test stage of system life cycle), for training individuals or for research purposes. |
| **PIA 28:** | Identify legal authorities, governing information use and disclosure specific to the system and program. | The FDA has authority to collect and use adverse event related data under provisions of the Food, Drug, and Cosmetic Act, 21 U.S.C. 301, including sections 353, 356b, 360; and the Public Health Service Act, 42 U.S.C. 201 including sections 262, 263a. |
| **PIA 29:** | Are records in the system retrieved by one or more PII data elements? | No |
| **PIA 30:** | Identify the sources of PII in the system. | Non-Government Sources<br>Other |
| **PIA 30A:** | Identify the “other” sources of PII in the system not mentioned in the above list. | eHealth Exchange Network |
| **PIA 31:** | Is there an Office of Management and Budget (OMB) information collection approval number? | No |

| | | |
|---|---|---|
| **PIA 31B:** | Explain why an OMB information collection approval number is not required. | The BEST Platform is only being used internally by FDA employees and BEST direct contractors. The data collected are from an existing, non-government system and is not acquired through an information collection as defined under the PRA. |
| **PIA 32:** | Is the PII in the system shared directly with other organizations outside the system's Operating Division? | No |
| **PIA 33:** | Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act? | Voluntary |
| **PIA 34:** | Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why. | There is no opportunity for individuals to opt-out as all PII is obtained from previous collections and not from individuals directly. The organization conducting the initial collection would be responsible for obtaining any required consent and providing opt-out mechanisms. |
| **PIA 35:** | 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). If they cannot be notified or have their consent obtained, explain why. | If FDA changes the collection, use, or sharing of PII data in this system, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on an FDA web site, e-mail notice to the individuals, inclusion in newsletters, or information provided to supervisors with instructions to further inform staff. However, no such changes that would affect the rights or interests of the individuals are anticipated. |
| **PIA 36:** | 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 FDA system have many avenues available for assistance. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and other agency offices, via email, phone and standard mail avenues (all listed on FDA.gov and the FDA intranet).<br><br>In the event of a suspected incident or data breach, FDA personnel must report that without delay to the FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). |
| **PIA 37:** | Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not. | Data reviews and the data integrity, availability, accuracy and relevancy is addressed in the context of the source system. These processes are not necessary to be duplicated as part of the PS & S CBER Biologics Effectiveness and Safety (BEST) Platform. |
| **PIA 38:** | Identify who will have access to the PII in the system. | Users<br><br>Contractors |
| **PIA 38A:** | Select the type of contractor. | HHS/OpDiv Direct Contractors |

| | | |
|---|---|---|
| **PIA 38B:** | Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices? | Yes |
| **PIA 39:** | Provide the reason why each of the groups identified in 38 needs access to PII. | CBER Subject Matter Experts (personnel) need access to the data to evaluate if the quality of the data received by the FHIR interface is adequate for medical review for regulatory purposes. The PII itself is not as relevant as the overall granularity and breadth of the data.<br>Contractors may review the data in determining completeness of extracts and to ensure data is being ingested correctly. |
| **PIA 40:** | Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII. | The administrative procedures in place to determine which system users may access PII are the standard processes FDA employs to onboard new employees and contractors. Supervisors, managers and/or other officials approve access via documented administrative process (e.g., access request forms). Access permissions and scope are designated at the individual level limiting access based on an individual's role and authorized need. All users of the PS & S CBER Biologics Effectiveness and Safety (BEST) Platform will be fully vetted and badged FDA employees and contractors. Technical controls are applied based on individual roles and duties to ensure only individuals with a need to know are granted access to the pilot system. |
| **PIA 41:** | Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job. | The following technical methods are in place to allow those with access to PII to only access the minimum amount of information necessary to perform the job: Users must log into the system with their credentials. Each user is given a role when access to the system is granted. Users are given ROLES that permit access only to specific types of information (Role based access control RBAC).<br><br>The platform will use one of the approved protocols for single sign on (SSO) multifatcor authentication and authorization to ensure that the user accesses only the minimum amount of information necessary to perform their job. PINGFED, one of the potential SSO methods, is a private sector owned authentication authority operating a federation server that provides identity management and security support. |
| **PIA 42:** | Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained. | All users and administrators of the PS & S CBER Biologics Effectiveness and Safety (BEST) Platform are required to complete the following training and awareness programs to make them aware of security practices and protecting PII.<br>All FDA personnel complete mandatory security and privacy awareness training at a minimum of once a year. |
| **PIA 43:** | Describe the training system users receive above and beyond general security and privacy awareness training. | BEST platform specific training. |

| | | |
|---|---|---|
| **PIA 44:** | Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s). | For the project files:<br>File Code: FDA-9991a2<br>NARA Authority: GRS 3.1, item 011<br>Title: Information Technology Development Project Records: System development records<br>Disposition: TEMPORARY. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.<br>For the system itself:<br><br>File Code: FDA-9997<br>NARA Authority: GRS 3.1, item 012<br>Title: Information Technology Development Project Records: Special purpose computer programs and applications<br>Disposition: TEMPORARY. Delete when related master file or database has been deleted, but longer retention is authorized if required for business use. |
| **PIA 45:** | Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response. | FDA secures PII in the system using the following administrative controls: Users must request accounts and access to the BEST Platform and be fully vetted and badged prior to receiving access.<br><br>FDA secures PII in the system using the following technical controls: Access to the servers and application is managed through assigned and vetted user accounts and logins using SSO, PINGFED, and KeyCloak technology.<br><br>FDA employs network firewalls, encryption and other technical methods at the system and network levels. Applied physical controls include secure monitored guarded facilities. |

## Review and Comments

### OpDiv Privacy Analyst Review

| | | | |
|---|---|---|---|
| **Privacy Analyst Review Decision:** | Approved | **Privacy Analyst Review Date:** | 8/12/2025 |
| **Privacy Analyst Review Comments:** | | **# of Days - PA Review:** | 0 |

### SOP Review

| | | | |
|---|---|---|---|
| **SOP Review Decision:** | Approved | **SOP Review Date:** | 8/12/2025 |
| **SOP Review 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. | **# of Days - SOP Review:** | 0 |

### Agency Privacy Analyst Review

| | | | |
|---|---|---|---|
| **Agency Privacy Analyst Review Decision:** | Approved | **Agency Privacy Analyst Review Date:** | 8/21/2025 |
| **Agency Privacy Analyst Review Comments:** | Reviewer: Crystal Bland<br><br>8/21/2025 This PIA is ready for SAOP review and approval. | **# of Days - APA Review:** | 9 |

### SAOP Review

| | | | |
|---|---|---|---|
| **SAOP Review Decision:** | Approved | **SAOP Review Date:** | 8/29/2025 |
| **SAOP Review Comments:** | | **# of Days - SAOP Review:** | 8 |

#### SAOP Signature

| Date | User | Type | Name | Original Value | New Value |
|---|---|---|---|---|---|
| 8/29/2025 1:48 PM | BAUR, VANESSA | Signature | SAOP (Email PIN) | | Content Signed |

### Supporting Document(s)

| Name | Size | Type | Upload Date | Downloads |
|---|---|---|---|---|
| No Records Found | | | | |

## Comments

| Question Name | Submitter | Date | Comment | Attachment |
|---|---|---|---|---|
| PTA 01 | BLAND, CRYSTAL | 8/13/2025 | 8/13/2025 Per FDA's Email:<br><br>This PIA was externally approved by HHS on 12/6/2024 but needed to be entered in Archer because of a sync issue.<br><br>The planned ATO date is 12/31/2025. | 8-13-2025 EMAIL_PIA in Queue (CBER Biologics Effectiveness and Safety).pdf<br><br>BEST_PTA_PIA_12-6-2024_SAOP Approved.docx<br><br>CBER Biologics Effectiveness and Safety_SOP Approved 8.12.2025.pdf |