PTA / PIA: FDA - BIRAMS - QTR3 - 2025 - FDA4955920

Created Date: 8/29/2025 12:42 PM Last Updated: 9/9/2025 4:25 PM

General Information

PTA / PIA Name:	FDA - BIRAMS - QTR3 - 2025 - FDA4955920	**PTA / PIA ID:**	3728578
Component Name:	FDA - CBER Biologics Investigational and Related Application Management Systems	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	13
Submitter:		**Submit Date:**	8/29/2025
Next Assessment Date:	09/08/2028	**Expiration Date:**	9/8/2028
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
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.	11/21/2022
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	Christopher Kiem
PTA 01A:	POC Title and Organization	POC Title: Business Owner POC Organization: FDA/CBER
PTA 01B:	POC Email Address	Christopher.kiem@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-8093
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 Food and Drug Administration (FDA) Center for Biologics Evaluation and Research (CBER) regulate biological products for human use under applicable federal laws, including the Public Health Service Act and the Federal Food, Drug and Cosmetic Act (FDC&A). The CBER Office of Regulatory Operations (ORO) system is made up of multiple components/modules that support CBER's mission to protect and enhance the public health. CBER ORO interfaces with its components/modules for document tracking and routing, reporting, Investigational New Drug Tracking (IND) applications, Blood Logging and Tracking (BLT), Electronic Submissions (CER), Lot Release (LRS), Biologics Investigational and Related Application Management tracking and summarization, maintenance of valid person names and associated information, and Post Market safety surveillance activities. The subject of this assessment is the Biologics Investigational and Related Application Management System (BIRAMS). CBER BIRAMS supports high-level tracking and summarization of CBER regulatory efforts associated with Investigational New Drug applications (INDs), Master Files (MF), and Investigational Device Exemptions (IDEs). Emergency Use Authorizations (EUAs) are also supported. CBER BIRAMS has Report Generators for report listings, routing screens and routing reports for IND management, and is integrated with CBER's Electronic Document Room (CER, the subject of a separate assessment). CER has electronic IND document routing, electronic signatures on IND internal documents, electronic forms for reviewers' data management, and portable document formats (PDFs) of IND documents. CBER BIRAMS users include FDA employees and Direct Contractors.
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.	CBER BIRAMS does not collect personally identifiable information (PII) about FDA employees, Direct Contractors, sponsors, or holders (submitters). However, the system may maintain the PII of patients or clinical trial subjects who have voluntarily disclosed this information although not solicited by FDA (e.g., adverse event reporting). This information may include name, email address, telephone number, fax number, and mailing address. telephone number. Information may also include professional credentials (e.g., PhD, MD) and business contact information (name, email, telephone number, and mailing address) for points of contact at regulated entities. Information handled in this system consists of submissions seeking various FDA approvals. An Investigational New Drug Application (IND) is a request for FDA to permit the applicant to administer an investigational drug or biological product to humans. Such authorization must be

secured prior to interstate shipment and administration of any new drug or biological product that is not the subject of an approved New Drug Application (NDA) or Biologics/Product License Application (BLA). An investigational device exemption (IDE) allows the investigational device to be used in a clinical study to collect safety and effectiveness data. A “510(k)” submission is a premarket submission to FDA to demonstrate that the device to be marketed is substantially equivalent to (at least as safe and effective) a legally marketed device that is not subject to a pre-market approval, which requires submitters to compare their device to one or more similar legally marketed devices to support their substantial equivalency claims. A drug/device master file (DMF) is a confidential, detailed document submitted to the FDA by Active Pharmaceutical Ingredient (API) manufacturers. A DMF contains the chemistry, manufacturing, and controls of a drug component or the product (e.g., ingredient, subassembly, or accessory) or facility in the manufacture of the device. The information in a DMF may be used to support other submissions such as an IND or NDA.

Another type of submission is a request for an Emergency Use Authorization (EUA). Per the FDC&A, FDA strives to protect against chemical, biological, or radiological/nuclear agent (CBRN) threats by facilitating the availability and use of Medical Countermeasures (MCMs) during public health emergencies. By law, the FDA Commissioner may allow unapproved medical products or unapproved uses of approved medical products to be used in an emergency to diagnose, treat, or prevent serious or life-threatening diseases or conditions caused by CBRN threat agents when there are no adequate, approved, and available alternatives.

A “Blood Variance Request” is a petition for exemption from requirements (methods, facilities, controls) proposed for the manufacture, packing, storage, and use of a blood product, to ensure the product will be safe and effective for public consumption; a Blood Donor Requalification is a request to allow a previously deferred donor to donate blood if the donor meets the eligibility criteria. The request is submitted to the FDA for approval along with supporting documents and test results.

All data collected in the 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. All users are authorized full time FDA employees and Direct Contractors with FDA badges and smart cards. Access to this system is granted through the CBER

		Menu application via FDA's Single Sign-On (SSO) process.
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.	CBER BIRAMS does not collect or share any PII. CBER BIRAMS may maintain PII of patients or clinical trial subjects who of their own initiative opt to voluntarily provide PII not solicited by FDA (e.g., when submitting an adverse event report). The system may maintain the PII of patients or clinical trial subjects who have voluntarily disclosed this information although not solicited by FDA (e.g., adverse event reporting). This information may include name, email address, telephone number, fax number, and mailing address. telephone number. Information may also include professional credentials (e.g., PhD, MD) and business contact information (name, email, telephone number, and mailing address) for points of contact at regulated entities. CBER BIRAMS provides electronic bridges to existing databases and documents. Users of CBER BIRAMS (FDA employees and Direct Contractors) access the website via an internal uniform resource locator (URL) and FDA's Single Sign-On authentication process. CBER BIRAMS interfaces with the following CBER applications: Regulatory Management System – Biologics Licensing Application (RMS-BLA), Document Accountability Tracking System (DATS), CBER Regulatory Meetings Tracking System (CRMTS), Pre-Application Tracking System (PTS), CBER Connect, CBER Electronic Repository (CER), CBER Activity Time Tracking System (BITS-CATTS), and Animal Components Database (ACD). In addition, CBER BIRAMS interfaces with the Food and Drug Administration Office of Regulatory Affairs (FDA/ORA) Mission Accomplishments and Regulatory Compliance Services (MARCS) Center Views. Information handled in this system consists of submissions seeking various FDA approvals, including INDs, NDAs, BLAs, IDEs, 510(k), DMFs, EUAs, Blood Variance Requests, and Blood Donor Requalification. The data is reviewed by FDA as part of the product approval process. Adverse event reporting such as individual case safety reports (ICSRs) and other post-marketing safety surveillance requirements are submitted to FDA before and after a marketing applications approval.
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).	http://cberforms.fda.gov/forms/cber_images/cbermenu.html
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 BIRAMS users with access to existing databases and documents. Users of CBER BIRAMS (FDA employees and Direct Contractors) access the website via an internal URL and FDA's SSO authentication process.
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?	No
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 Name Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Fax number, Professional credentials (e.g., PhD, MD).
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Patients Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100,000 – 999,999

PIA 25:	For what primary purpose is the PII used?	If provided, this information is used to contact people to clarify data regarding their submissions and to assist in follow-up analysis of the data.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	The FDA makes no secondary use of the PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The legal authorities governing information use and disclosure include Title 21 Code of Federal Regulations (CFR) part 312; Title 21CFR part 812; Title 21CFR parts 814.3 & 314.420; Title 21 sections 564, 564A, and 564B of the Federal Food, Drug, and Cosmetic Act (FD&C Act) as amended and added by the Pandemic and All-Hazards Preparedness Reauthorization Act of 2013 (PAHPRA); Title 21 CFR parts 600-680; Title 21 CFR parts 640.120; and 5 U.S.C. 301. In addition, the security and privacy measures of the applications are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.
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.	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Email Online Government Sources Other HHS OPDIV State/Local/Tribal Foreign Non-Government Sources Members of the Public Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	0910-0014 expires 09/30/2026 0910-0001 expires 8/31/2028
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 method for employees to opt-out of submitting their PII. Permanent FDA employees and Direct Contractors must provide their PII in order for the Agency to process administrative materials and securely administer access to Agency information and property. External individuals submitting comments to the Federal Register are not mandated to submit any PII. External individual (non-employees) submitters were notified on forms they submitted (no longer in use), in Federal Register publications (e.g., comment submission guidance and SORNs), privacy statements on the FDA.gov and in other resources provided on FDA.gov. FDA's Federal Register notices inform individuals of the procedures for commenting on a notice and advise that submitted comments may be made public.
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 a major change in the collection, use or sharing of PII data for this application occurs, users will be notified via individual e-mail notification, FDA wide e-mail and/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 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.	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. Any changes to an individual's name or address would need to be updated using a Standard Form 50 or 52, which is the process used to make such changes used by all FDA employees, and the data would be updated in the separate human resources information system. External individuals 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 incidents or breaches to the FDA CIOCC. Contractors are required to safeguard all information and to report potential data breaches to the FDA.

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.	Any patient PII provided by the individual is do submitted on a voluntary basis. 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 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 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 38:	Identify who will have access to the PII in the system.	Users Administrators Developers 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.	Users-require access to the system in order to track and monitor submissions for regulatory approval. Note that "users" may include subject individuals, supervisors, or business function administrators. Administrators- May be application administrators who require access to conduct business functions, or application administrators who require access to create and manage user accounts for specific applications. Developers-will not normally have access to PII but may in the course of maintaining the systems or providing technical assistance. Contractors - Some developers may be Direct Contractors and will have access under the same circumstances as developers.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA employees and Direct Contractors who require access to the application need to have supervisor approval and sign off 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 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.	All users including administrators, developers, and Direct Contractors are granted only the minimal privileges required to do their job. User supervisors indicate on the account creation form the minimum system access that is required, and these minimum access restrictions are enforced through technical system settings and individual identity and role authentication processes such as multifactor authentication (MFA). All users are FDA network users and must have a current Personal Identity Verification (PIV) compliant badge.
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 system users at FDA must complete 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 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Help links are available within applications, and instructional materials are available on the FDA intranet for all applications. All users are instructed on adhering to the HHS Rules of Behavior in the context of their work involving this system. For additional privacy guidance, personnel may contact the Agency's privacy office. Privacy program materials are provided to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA.

PIA 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).	All Adverse Event files are temporary, and destroyed according to the instructions cited in the following records schedules: FDA 5, Adverse Event/Experience and Product Defect Reports; 5.1, Adverse Event Reports Management Files; 5.2, Adverse Event Reports or Forms; 5.3, Adverse Event Reporting Systems; 5.3.2, AERS Database Records; 5.3.3, Extracts of the Adverse Event Data for Public Access: Output Records; General Records Schedule (GRS) 5.1 and 5.2, Electronic Records, Items 2a, 2b, 4, 5, 6, 7, 11a(1), 12, 16. CBER Records Control Schedule (NARA Schedule No. N1-088-03-05) Items B-34, Post Marketing Products Safety Reviews and Adverse Event Summaries, and B-35, Post-Marketing Surveillance Lot Analysis Reports. Records are retired to the Washington National Records Center three years after the cutoff date and destroyed 20 years after the cutoff date.
PIA 45:	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 NIST Special Publication 800-53, as determined using FIPS199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	8/29/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	8/29/2025
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:**	9/3/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 9/3/2025 Comments have been addressed. This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	5

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	9/9/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	6

SAOP Signature

Date	User	Type	Name	Original Value	New Value
9/9/2025 3:06 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
PIA 22	BLAND, CRYSTAL	9/3/2025	9/3/2025 The correct ATO Date is 8/3/2025.	9-3-2025 BIRAMS ATO.pdf