Privacy Impact Assessment (PIA): FDA - BITS-COMP - QTR4 - 2024 - FDA4899295

Created Date: 12/4/2024 11:21 AM Last Updated: 12/6/2024 2:50 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 - BITS-COMP - QTR4 - 2024 - FDA4899295	**PIA ID:**	2511306
Name of Component:	FDA - CBER Biologics Information Tracking System - Compliance	**Name of ATO Boundary:**	CBER Office of Regulatory Operations
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	3
Submission Status:	Submitted	**Submit Date:**	12/4/2024
Next Assessment Date:	N/A	**Expiration Date:**	12/6/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4899295
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
2:	Is this a FISMA-Reportable system?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	11/21/2022
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
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 Center for Biologics Evaluation and Research (CBER) Biologics Information Tracking System-Compliance (BITS-COMP) technology is used to track the capture and processing of complaints and inspections associated with CBER's Office of Compliance and Biologics Quality (OCBQ). CBER BITS-COMP is one of many pieces of technology operating under the CBER Office of Regulatory Operations (ORO) system boundary. Other technology, systems and components within ORO are assessed separately. The Food and Drug Administration (FDA) previously assessed BITS-COMP in conjunction with other elements of ORO and is now conducting this assessment to supplement previous assessments and ensure transparency. ORO supports CBER's mission to protect and enhance the public health through the regulation of biological and related products (e.g., blood, vaccines, allergenics, tissues, cellular and gene therapies) and tracking of Post Marketing Commitments related to these approved products. A wide range of users at CBER and the FDA utilize CBER ORO and the system's associated components and tools to support the FDA/CBER mission. Users include Regulatory Information Specialists, Consumer Safety Officers, Information Technology Specialists, Administrative Officers, Management Analysts, Reviewers, and Medical Officers. CBER ORO is housed in the FDA's Ashburn Data Center (ADC) which is operated by Peraton contractors. CBER Systems Operations and Modernization (CSOM) contract staff administers the CBER ORO application, and Peraton provides data center and infrastructure support. Peraton provides information technology hosting services to support FDA applications/ components. It is a "lights out" facility, meaning all administration, maintenance and other operational management is done remotely with only facility personnel being physically located at the ADC facility on a continuous basis. System users include FDA Permanent employees and Direct Contractors. Users' login to BITS-COMP via the internal website uniform resource locator (URL) and verify their identity through Single-Sign On (SSO) multi-factor authentication.

PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	CBER BITS-COMP collects personally identifiable information (PII) about companies and individuals submitting complaints or inspections data. Reporters submit this information via email, phone or traditional mail-in method. PII consists of submitter name and address as required, and other optional fields like address, phone number, email address, FDA Establishment Identifier (FEI), Data Universal Number System (DUNS) number, and firm information. The types of data that are maintained in the system are complaints data and inspections information, as well as communications lists and information regarding communication review committee actions. There is no downstream system for BITS-COMP. Complaint and inspection files involving adverse events (e.g., reactions to a vaccine) are temporary, and destroyed according to the instructions cited in the applicable records schedules. Additional records are maintained under CBER Records Control Schedule N1-088-03-05 (National Archives and Records Administration (NARA) approved) 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.
PTA - 5A:	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. The system providing credentials is
PTA - 5B:	Please identify the type of user credentials used to access the system.	
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.	The BITS-COMP module tracks the capture and processing of complaints and inspections related to CBER's Office of Compliance and Biologics Quality (OCBQ). Company, individual and firm information and associated PII is collected and maintained to track the source of the complaint or inspection, as well as identify the subject of the complaint or inspection. This PII is necessary to enable the FDA to accurately assess submissions and conduct follow up efforts to ensure public health and safety. PII in BITS-COMP is not shared outside the FDA and internally no PII in BITS-COMP flows down to other systems.
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.	BITS-COMP has an FDA CBER internal website that is used to track the capture and processing of complaints and inspections related to CBER's Office of Compliance and Biologics Quality (OCBQ). Only CBER fulltime permanent employees (FTEs) and Direct Contractors with specific access and role can access the system. The categories of individuals who have access to the website are those responsible for data entry, reviewers, and administrators. Users' login to BITS-COMP via the internal website uniform resource locator (URL) and verify their identity through Single-Sign On (SSO) multi-factor authentication.
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 Others - Chart No., TIN, DUNS, Provider License #
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 FDA uses the PII in BITS-COMP for the primary purpose of tracking the individual, company or firm submitting a complaint or inspection data and the individual or entity associated with the complaint.
PIA - 5:	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 - 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 implementation of this application is authorized by 5 U.S.C. 301, Federal Food, Drug and Cosmetic Act, 21 USC 353, 356b, 360; and the Public Health Service Act, 42 USC 263a. In addition, the security and privacy measures of the applications are required by the Federal Information Security Modernization Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Phone Email Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	

PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	An OMB information collection approval number is not required because this is not a Paperwork Reduction Act information collection. There are no associated forms associated with CBER BITS-COMP.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	PII is provided to aid in communications and is "voluntary" as that term is used by the Privacy Act. There is no method for individuals to opt out of submitting their PII. While submission is "voluntary" as that term is used by the Privacy Act, the PII is necessary for FDA actions such as tracking submissions and following up with a complaint submitter.
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 for this application occurs, users will be notified via individual email notification or in updated notice statements on submission forms and Federal Register publications. However, no such changes that would affect the rights or interests of the individuals are anticipated.
PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Individuals who suspect their PII has been inappropriately obtained, used, or disclosed may contact agency offices, via email, phone, and standard mail avenues (all listed on FDA.gov and the FDA intranet). The FDA Privacy Office provides its contact information on FDA.gov. In the event of a suspected incident or data breach, FDA personnel must report that without delay to the FDA's CIOCC.

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.	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. FDA personnel may correct/update information discovered to be incorrect. 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 when providing the system with an authorization to operate (ATO). Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. CBER performs annual reviews to evaluate user access. One of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified during system use are addressed when discovered.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: Require access to the system to create, update and perform routine tasks pertaining to their job responsibilities using the systems granted access to. 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 while 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 - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and Direct Contractors with valid network accounts who require access to the system must obtain supervisory approval and signature before access is granted. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system.

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.	All users including administrators, developers, and Direct Contractors are granted only the minimal privileges that they require to do their job. The users' supervisor indicates on the account creation form the minimum system access that is required. All users are FDA network users and must have a current Personal Identity Verification (PIV) compliant badge.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.	All system users at FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity, and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Digital Transformation (ODT) verifies that training has been successfully completed.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	System users receive system-specific training, review the HHS Rules of Behavior. Additional role-based training on privacy is available via FDA's privacy office.
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).	Complaint and inspection files involving adverse events (e.g., reactions to a vaccine) 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 5.22 Electronic Records, Items 2a, 2b, 4, 5, 6, 7, 11a(1), 12, 16. Permanent records are maintained in other systems. Additional records are maintained under CBER Records Control Schedule N1-088-03-05 (National Archives and Records Administration (NARA) approved) 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 - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from NIST Special Publication 800-53, as determined using FIPS199.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	12/4/2024
Privacy Analyst Comments:	Added externally approved PIA to Archer (attached).	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	The FDA's Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls. Externally approved by SAOP 7.23.2024	**SOP Review Date:**	12/4/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	12/5/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 12/5/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	There are 2 Archer issues impacting this PIA. The Answer to PTA-5A is entered on the PTA but does not show on the PIA. PTA-5A, Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is Active Directory. This PIA is also experiencing an Archer error with Question #3 of the general information. Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)? The FDA instance of Archer is reflecting “No” as the answer when the correct answer is “Yes.” The FDA Archer Team is aware of this occurrence and is working on a solution. The FDA Archer Team is aware of this occurrence and is working on a solution.	**SAOP Review Date:**	12/6/2024
		SAOP Days Open:	1

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
12-4-2024 EMAIL_PIA in Queue (CBER Biologics Information Tracking System - Compliance).pdf	1154437	.pdf	12/4/2024 1:34 PM	0
CBER Biologics Information Tracking System - Compliance_SOP Approved.rtf	784266	.rtf	12/4/2024 1:34 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	12/5/2024	Per FDA's Email: There are 2 Archer issues impacting this PIA. The Answer to PTA-5A is entered on the PTA but does not show on the PIA. PTA-5A, Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is Active Directory. This PIA is also experiencing an Archer error with Question #3 of the general information. Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)? The FDA instance of Archer is reflecting “No” as the answer when the correct answer is “Yes.” The FDA Archer Team is aware of this occurrence and is working on a solution. The FDA Archer Team is aware of this occurrence and is working on a solution.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	12/6/2024 2:50 PM	**History Log:**	View History Log