PTA / PIA: FDA - Sentinel - QTR4 - 2025 - FDA5079500

Created Date: 12/8/2025 11:23 AM Last Updated: 12/22/2025 3:42 PM

General Information

PTA / PIA Name:	FDA - Sentinel - QTR4 - 2025 - FDA5079500	**PTA / PIA ID:**	4102820
Component Name:	FDA - CDER Sentinel	**ATO Boundary Name:**	CDER Sentinel
Overall Status:	Complete	**# of Days - Open:**	14
Submitter:		**Submit Date:**	12/8/2025
Next Assessment Date:	12/21/2028	**Expiration Date:**	12/21/2028
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.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	4/18/2025
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Rhoda Eniafe
PTA 01A:	POC Title and Organization	System Owner
PTA 01B:	POC Email Address	Rhoda.Eniafe@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-9915
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	Significant System Management Change

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The Center for Drug Evaluation and Research (CDER) Sentinel System is transferring the hosting environment from MS Azure to Amazon Web Service (AWS) East.
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 CDER Sentinel System (hereafter referred to as "Sentinel") is a project sponsored by the U.S. Food and Drug Administration (FDA) as part of an initiative to create an active safety surveillance system called the Sentinel System to monitor the safety of FDA-approved medical products. To accomplish this purpose, Sentinel uses pre-existing electronic healthcare data provided by multiple sources. The overarching Sentinel Initiative is the FDA's response to the Food and Drug Administration Amendments Act of 2007 (FDAAA) requirement that the FDA work with public, academia, and private entities to develop a system to obtain relevant information from existing electronic health care data in order to assess the safety of approved medical products.

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.	Sentinel uses pre-existing, de-identified electronic healthcare data from the various Sentinel Data Partners. Data Partners include participating health insurers, care providers and academic institutions. Initial data queries developed by FDA analysts are provided to the Data Partners and they provide responses in de-identified, summary format to an Operations Center which aggregates the data and provides it to the FDA. A contractor, Biswas Information Technology Solutions (BITS) (hereafter referred to as BITS) operates Sentinel and specifically, the Operations Center. BITS contractors are direct contractors with FDA credentials. Most Sentinel activities focus on safety assessments, evaluation methods, or data. The fact that FDA requests and receives data on a particular product through Sentinel does not necessarily mean there is a safety issue with the product. By design, all data providers must de-identify any data (remove direct patient/person identifiers) before providing it to the Operations Center. The Operations Center subsequently transmits de-identified information to FDA in response to queries submitted by FDA. In the event that person-level information (as opposed to more typical aggregated or cumulative data) is required for FDA analyses, Data Partners remove direct patient/person identifiers from the information conveyed to the Operations Center. If the Operations Center inadvertently receives direct patient identifiers, it will return or destroy the data immediately. All data that FDA receives is intended to be thoroughly de-identified before it reaches FDA. When submitting data requests (aka queries), FDA users access Sentinel using their system credentials (Internal FDA users - Personal Identity Verification (PIV) and Personal Identification Number (PIN), External users (email and password). In order to register for an account, users must submit an Access Request form, providing their first name, last name and e-mail address for FDA Approval, and the system will auto-generate the user account to access the system and provide access to identified areas including the Sentinel Portal. Administrators are responsible for verifying access to system designated approved areas for FDA employees and direct contractors. The system auto-generates a password for external users which is masked within the PostgreSQL database (DB) in AWS East (a FEDRAMP compliant hosting environment that is subject to a separate PIA) with DB encryption on the password field.
PTA 05A:	Are user credentials used to access the system?	Yes

PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Email Address Non-HHS User Credentials Username Password
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 Sentinel project provides FDA the ability to (1) work through the nuts and bolts of designing safety assessments using multiple existing electronic healthcare data systems; (2) develop and evaluate scientific methods to increase the precision of active health and safety surveillance efforts; and (3) identify and address barriers and challenges to building a practical, accurate, and timely system for active safety surveillance. Sentinel uses de- identified pre-existing electronic healthcare data from multiple sources (the Data Partners). FDA may access the data available through Sentinel for a variety of reasons beyond assessing potential safety risks for a specific product. Some examples include determining a rate or count of an identified health outcome of interest, examining medical product use, or seeking to better understand the capabilities of the Sentinel project. Sentinel employs a distributed data approach in which the individual Data Partner entities maintain physical and operational control over electronic data in their existing environments. This approach minimizes the need to share identifiable patient information. Additionally, each health care data system has unique characteristics, and use of a distributed system enables the Data Partners to perform analyses in their environment. By virtue of this process, unique system characteristics do not present a technical roadblock or require system redesign. The distributed data model thereby ensures an informed approach to interpreting queries and analytical results across multiple Data Partners. The Operations Center coordinates all activities and queries with the Data Partners. FDA submits queries to the Operations Center which prepares and sends the appropriate analytical program that each Data Partner will run behind its own firewall. Each Data Partner will then submit de- identified aggregated results to the Operations Center. The Operations Center aggregates the data from each of the Data Partners and sends a final aggregated data report to the FDA. After the report has been finalized, it is posted on sentinelsystem.org. Data transfer between Data Partners and the Operations Center, and, between the Operations Center and the FDA is done by means of a secure web-based file sharing system. When submitting data requests, FDA users access Sentinel using system-specific usernames and passwords. Users must provide a first name, last name and e-mail address in the processes of creating an account to the Sentinel portal. Users create their own passwords that must meet

		complexity standards. Administrators are responsible for creating Sentinel user accounts for FDA employees and direct contractors. The information about users is collected and/or maintained in order to determine if they have approval to access the system. Personally Identifiable Information (PII) from the system/component/collection is shared with FDA Contracting Officer's Representative (COR) and their assigned key personnel in order to approve access to the system to maintain the proper user base.
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://Sentinel-Platform.org https:/SentinelInitiative.org
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes
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.	Users accessing the internal website are presented with the FDA System Warning and prompted to log in. This internal website facilitates collaboration between FDA Employees and Direct Contractors and Data Partners. User authentication is handled through a combination of this system and FDA's internal ICAM (Identity, Credential, and Access Management) system. No login is necessary for the public website.
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.	Other technology - Does Not Collect PII
PTA 12B:	What other technology is used?	Sentinel uses Google Analytics to gather user metrics.
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?	Yes

PTA 21A:	What are the AI tools and how are they used?	Google Analytics is considered both a machine learning and AI tool because it uses machine learning algorithms to power its AI features. Sentinel uses Google Analytics to gather user metrics. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.

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 User Credentials Contact Information Email Address (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100 – 499
PIA 25:	For what primary purpose is the PII used?	The FDA uses the PII for the primary purpose of authenticating users.
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 that govern information use and disclosures specific to the system and program are: The Food and Drug Administration Amendments Act of 2007 (FDAAA) amended the Federal Food, Drugs and Cosmetics Act to require the FDA to establish collaborations with public, academic, and private entities to provide for advanced analysis of drug safety data and other information that is publicly available or is provided by U.S. Department of Health and Human Services (HHS) and partners to its initiatives. Further, the FDAAA specifies that such analysis shall not disclose individually identifiable health information when presenting such drug safety signals and trends or when responding to inquiries regarding such drug safety signals and trends.' (See 21 U.S.C. 505(k)(4)(A) and (B).)
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 Email Government Sources Within the OPDIV

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.	This component does not collect information using an information collection request as defined by the Paperwork Reduction Act.
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.	The submission of PII is voluntary, meaning individuals cannot be legally forced to provide it, however, PII is functionally required for system access. Users cannot access or use the system without submitting PII, and no opt-out mechanism exists. FDA employees, direct contractors, and data partners must provide their PII to facilitate administrative processing and maintain secure access to agency information and property, including the Sentinel system.
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.	No such changes are anticipated. If the agency 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 the web site, or e-mail notice to the individuals. Because the health data in this system is thoroughly de-identified, notification would not be possible.
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 a number of avenues available to request to rectify the situation. Often, these individuals contact the office or division where they have determined that their information is held. Individuals may then make further requests for their information to be corrected or amended. FDA considers these requests and, if appropriate, makes the requested changes. Employees with such concerns can additionally work with their supervisors, a 24-hour technical assistance line, and 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.	Because data providers de-identify the information before providing it the Operations Center and FDA, no reference model is available to FDA to facilitate re-assessing data integrity. Potential data integrity issues would be addressed by the source, i.e., the data providers. All internal users (FDA Employees and Direct Contractors) of this application are responsible for providing accurate information and may independently update and correct their information at any time. Additionally, accuracy is ensured by reviewing PII Quarterly for User Accuracy Reporting (UAR) and at least bi-weekly review and validation of user logs. All information is relevant to the authentication and authorization process. Integrity and availability are protected by security safeguards selected based on guidance from the National Institute of Standards and Technology (NIST) appropriate to the level of risk associated with the application
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.	The reason the following groups need access to PII is: Users: Users have access to their own system login credentials (username and password). Users will not have access to others' login credentials. Administrators: Administrators may be application administrators who require access to create and manage user accounts but will not have access to users' self- created passwords. Developers: Developers may have limited access to usernames 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. BITS contractors will have access to user PII.

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: Only System Admins, Developers who may be contractors with full control of the system authorized by the FDA contracting officer's representative (COR) may access PII in order to support user authorizations, system auditing mandates and perform system updates.
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.	Management establishes roles for individual personnel, with role-based restrictions permitting access only to information that is required for each individual to perform his/her job. The user's passwords are masked.
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 CDER Sentinel users are required to complete annual mandatory Cybersecurity 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 (to include any special restriction on data use and/or disclosure). The FDA COR maintains copies of certificates and yearly training is done. The FDA Office of Digital Transformation (ODT) verifies and documents that FDA Employees and Direct Contractors have successfully completed this annual training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	No additional system-specific training is received by users; however, users are provided with user guides and manuals, and privacy guidance is available on the FDA intranet and from Privacy staff.
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).	The specific National Archives and Records Administration (NARA) records schedule and the retention schedule/retention period(s) is/are: General Records Schedule (GRS) 3.2. Item 030, Disposition Authority: DAA-GRS-2013-0006-0003. DISPOSITION: Temporary. Destroy when business use ceases.

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.	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 role-based access settings, firewalls, passwords and others. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology (NIST) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

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

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	12/8/2025
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:**	12/18/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 12/18/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	10

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	12/22/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	4

SAOP Signature

Date	User	Type	Name	Original Value	New Value
12/22/2025 1:02 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 21A	BLAND, CRYSTAL	12/18/2025	AI Review Completed	12-18-2025 CDC_FDA_RE_ AI Review Status_complete.pdf