PTA / PIA: FDA - CARS - QTR3 - 2025 - FDA4949333

Created Date: 7/16/2025 4:41 PM Last Updated: 7/17/2025 4:45 PM

General Information

PTA / PIA Name:	FDA - CARS - QTR3 - 2025 - FDA4949333	**PTA / PIA ID:**	3499615
Component Name:	FDA - CDRH Center Ad-hoc Reporting System	**ATO Boundary Name:**	CDRH Reporting and Collection Tools
Overall Status:	Complete	**# of Days - Open:**	1
Submitter:		**Submit Date:**	7/16/2025
Next Assessment Date:	07/16/2028	**Expiration Date:**	7/16/2028
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.	1/23/2023
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	Jonathan Adams
PTA 01A:	POC Title and Organization	Title: IT Specialist Organization: CDRH
PTA 01B:	POC Email Address	jonathan.adams@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-2604
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The United States of America (U.S.) Food and Drug Administration (FDA) has made no changes to this system/component since the last Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) was approved.
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 Center for Devices and Radiological Health (CDRH) Center Ad-hoc Reporting System (CARS) is an internal-facing application hosted in Ashburn Data Center (ADC) that leverages Oracle and Pentaho Data Integration software for business intelligence and data warehousing. CARS primary purpose is to provide CDRH with premarket and post-market business intelligence through ad hoc queries and report generation. The Premarket activity supported by CARS is mandated by the 1976 Medical Device Amendments to the Food, Drug and Cosmetic Act, the Medical Device User Fee and Modernization Act of 2002 (MDUFMA), and the FDA Amendments Act (FDAAA) of 2007. The post-market activities of CDRH are conducted under the authority of the Safe Medical Devices Act of 1991. CDRH and the Office of Inspections and Investigations (OII) personnel (FDA employees and Direct Contractors), require access to the data in the Center Ad Hoc Reporting System (CARS) data warehouse to perform their duties to track, approve, monitor, inspect, report, study, and recall medical device or radiation emitting products, and, to communicate with companies manufacturing such devices. A device can be either a medical device or radiation emitting product or both. Examples of medical devices include any device in a doctor's office, as well as implants, and diagnostic testing products such as glucose testing devices. Examples of both medical device and radiation emitting products include X-ray machines, Computed Tomography (CT) scanners, magnetic resonance imaging (MRI) machines, and dermatology and eye lasers. Examples of non-medical device radiation emitting products include lasers devices and microwave ovens. This data provides the ability to track the performance of devices and to make well informed decisions during the total life cycle of a device from premarket reviews through post-market monitoring, inspection, reporting, and recalling of a product from use. CDRH and OII use the Center Ad Hoc Reporting System (CARS) as a central data warehouse that receives personally identifiable information (PII) and non-PII metadata from multiple internal FDA systems. The CARS data warehouse system consists of a commercial off-the-shelf (COTS) front-end application, called Enterprise Business Objects which provides excel like reporting tools. The reporting tools interface with the CARS data warehouse using a secure web connection so users can generate reports.

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 CARS data warehouse collects PII and non-PII metadata from other internal FDA source systems. The PII and non-PII metadata collected from the FDA Source Systems include the Patients and medical device information from information submitted by Other Federal Agencies and or private companies. FDA employees and Direct Contractors review (FDA Reviewers) the information collected and correspond with external company contacts and/or representatives for more information. The PII contact data collected includes first and last name, mailing address, email address, and phone number. In addition, Federal contact information for assigned US Customs Agents, FDA inspector's and FDA Reviewers are also collected. This includes name, email address, and phone number. All contact information collected is professional/work contact information only. Device Identifiers are also collected by internal FDA systems. The CARS data warehouse also receives Patient Adverse Event data that includes Obfuscated Patient Identifier (MDR ID) along with the patient's Date of Birth, Weight, Sex, Age, Race, and Ethnicity. The non-PII metadata collected from source systems (listed elsewhere in this assessment) consists of medical nomenclature, product codes, reference data, facility information, information related to fees charged, facility inspection information, Adverse Event Reports (AERs) regarding medical device injuries and Medical Device Report (MDRs) failures, recall information, company registration, and product listing information. Source system AER and MDR content includes: the patient's age (patient being the individual who suffered the adverse event of a device failure), sex, weight, date of birth, race, and ethnicity and a system generated number (patient identifier) that uniquely identifies a specific patient on another system (encrypted MDR ID Number). Only this encrypted MDR ID Number is passed to CARS so as to mask or eliminate unnecessary replication of potentially identifying information. CDRH and OII personnel (permanent employees and Direct Contractors) do not use personal identifiers to retrieve data from CARS data warehouse.
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.	CDRH and OII personnel (FDA employees and Direct Contractors) use the data in relation to the agency's public health mission and medical device regulatory authority. This authority provides for reviewing and approving medical devices prior to their release for marketing and use, and, for conducting post-market safety surveillance activities, e.g., monitoring device usage problems

and adverse effects to identify trends and respond accordingly to ensure public health and safety.

The CDRH Ad-Hoc Reporting system, also known as the CARS data warehouse, imports data from the following internal FDA systems/tools: CDRH Entry System (CEntry); CDRH Center Tracking System (CTS); Medical Device Reporting System (eMDR); FDA's Unified Registration and Listing System/Device Registration and Listing Module (FURLS DRLM); Recalls Office of Regulatory Affairs Recall Enterprise System (ORA RES); Inspections OII's Field Accomplishments and Compliance Tracking System (FACTS); Device Nomenclature Management System (DNMS); CDRH Standards System (STDS); CDRH Radiological Health system (RH Pro); Global Unique Devise Identification Database (GUDID); Insight Time Reporting System (ITR); and Center Time Reporting System (CTRS).

These internal FDA source systems, briefly described below, are addressed in separate Privacy Impact Assessments (PIAs).

A single CARS Data Warehouse is maintained by CDRH. CDRH and OII management grants users' access to specific data based on individual user role/duties and their need-to-know. CDRH and OII staff all of which are FDA Employees and Direct Contractors who generate reports containing both PII and non-PII data as they contact and or correspond with representatives of or from medical device companies.

CDRH and OII's Direct Contractors which include FDA reviewers, FDA inspectors, FDA management, and FDA employees (CARS users) use data in the CARS data warehouse to support its public health mission to protect public health by approving the marketing of, sale and use of, and the adverse performance monitoring of medical or radiological devices. Users access to CARS through the SAP Enterprise Business Objects application via a network-level Single Sign-On process using their FDA Personal Identity Verification (PIV) cards for multi-factor authentication; CARS does not employ or maintain system-specific usernames, passwords or other access credentials.

CEntry captures documented medical device or radiation emitting product information sent by companies for regulatory approval. Data captured by CEntry includes product applicant/sponsor, correspondent, contacts, and third-party contact information for manufacturer representative, device trade name, decisions, comments, tracking, and maintains regulatory history of each change made to the original data captured in CEntry.

CTS is a workflow tracking system that captures product classification metadata, FDA Reviewer decisions, and captures each update or change as regulatory history on the review of CEntry

		documents. Medical Device Reporting system (eMDR) tracks Adverse Events Reports system (AERs) encountered with medical devices/radiation emitting device events (MDRs). Data captured by the MDR system provides specific manufacturer and product identification, malfunctions, injuries, deaths, manufacturer name, address, phone, email, and contact (information), reporting entity information, user facility information, and patient information via synthetic patient identity number (MDR ID) assigned to capture patient demographics, problems and outcomes. FURLS DRLM: Data captured by DRLM includes: Establishment (manufacturer) information FDA Establishment Identifier (FEI), data universal numbering system (DUNS) number, company name, address, uniform resource locator (URL), payment status, owner/operator information, correspondence information, US Agent information, listing information and regulatory history. OII's Recalls Enterprise System (RES) tracks the recall of products, firm information, manufacturer information, recall event information, consultant information, FDA recommendation, regulatory information. FACTS captures establishment Inspection information reports (EIRs), investigator information, firm information, inspection conclusion, recommendations, and reports.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	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.	Identifying Numbers Device Identifiers Biographical Information Name Date of Birth Contact Information 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.	Patient Age, weight, sex, race, and ethnicity Medical Device Request (MDR) ID Number (Obfuscated Patient Identifier) First and last names collected are representatives submitting or requesting information to and from the FDA, as well as US Customs Agents, FDA Inspectors, FDA Reviewers and Direct Contractors. All contact information collected is professional/work contact information only.
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 Patients
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?	CDRH and OII personnel (FDA employees and Direct Contractors) that review documents use the PII data from the Center Ad-hoc Reporting System (CARS) data warehouse to generate email correspondence to contact representatives for the company's providing submissions.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	Not applicable. No secondary uses for PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Federal Food, Drug, and Cosmetic Act, Section 519 (see 21 U.S.C. 360i).
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 Online 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.	The PIA(s) for any source system(s) would provide OMB approval numbers and expiration dates to the extent any of those systems collect information subject to 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.	CARS receives data from multiple source systems, each of which employs different methods or processes to notify individuals and ensure their awareness of the collection of their PII. The characteristics of the source systems and their notification methods are outside the boundaries of CDRH CARS (are not considered part of CARS). FDA conducts separate privacy assessments for the source systems. FDA personnel and Direct Contractors are notified at the time of hire of the agency's collection, creation and use of their PII in the context of their work performing government activities. At network logon prior to accessing the system, users view and acknowledge a displayed text window advising them that are using government systems and have no expectation of privacy. FDA's web and privacy policies are provided on all FDA internet (FDA.gov) and intranet (https://www.fda.gov/about-fda/about-website/website-policies) pages. This Privacy Impact Assessment provides further notice.
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 FDA changes its practices regarding the collection or handling of PII related to the CARS system, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.

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.	There is no complaint/notification process specific to CARS. External individuals may contact the FDA or CDRH by phone, mail or e-mail using the contact information provided on fda.gov to update or correct any information that is inaccurate. Internal and external individuals may also contact FDA's Privacy Office. Agency employees with concerns may seek assistance via FDA's Employee Resource Information Center (ERIC). 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, ERIC, the Cybersecurity 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). In the event of a suspected incident or data breach, FDA personnel must report that without delay to the FDA's 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.	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 their information themselves. PII relevancy is also ensured by design of the system to collect and maintain only that PII which is necessary for the intended purpose, e.g., communications and system access control. 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 in the course of providing the system with an authority to operate (ATO). Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. CDRH performs semi-annual reviews to evaluate user access.
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: For data analysis and reporting purposes. Some users are Direct Contractors. Administrators: Require access for system maintenance and administrative purposes. Some administrators are Direct Contractors. Developers: For development and support purposes. Some of the developers are Direct Contractors. Contractors: Direct contractors that provide development, support, maintenance and data analysis.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to CARS is given by default to all CDRH employees and Direct Contractors. FDA Enterprise Business Objects support team (FDA EBO) has a periodic process in place to compare the list of users who are given access to CARS with the list of CDRH users in the Active Directory and to add/remove users if necessary. Active Directory is the subject of a separate privacy assessment. If a user (newly hired) needs to get access to CARS immediately, they submit a help ticket to the Employee Resource and Information Center (ERIC) that is routed to the CDRH local Business Objects administrator.
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.	CDRH and OII developers, employees, and Direct Contractors are assigned role-based access to PII and non-PII in CARS on a need-to-know basis. User access to PII and non-PII data in the CARS data warehouse is reasonable and appropriate so access to specific data attributes is not restricted. A manager must submit a User Access Request Form to the CARS Help Desk for provisioning with the role-based access required for the user to perform duties.
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 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 Digital Technology (ODT) verifies that training has been successfully completed by FDA employees and Direct Contractors.
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 various CARS records are maintained under different National Archives Records Administration (NARA) citations as well as different FDA records schedules (also known as FDA File Codes). The records schedules for the different components of CARS are as follows: Premarket submissions (Premarket Notifications (510(k)), Premarket Approval (PMA), Modular PMA, Humanitarian Device Exemption (HDE), Investigational Device Exemption (IDE), Request for Information (513(g)), Pre-Submissions) are maintained with National Archives Records Administration (NARA) citation N1-088-08-1 items 2.2-items 2.5. For these, the disposition is temporary with the records being destroyed when final action is completed, when no longer needed for business use, or 25 years whichever is later. Various pre- and post- market reviews: Post Approval Study (PAS), Post Surveillance Study (PSS), Good Manufacturing Practices (GMP), and Bioresearch Monitoring (BIMO are maintained with NARA Citation N1-088-08-1 items 3.1 and 3.2. For PAS, PSS, GMP, and BIMO, the records disposition is temporary, and they are destroyed/deleted 30 years after cutoff or when no longer required for analysis. System for Uniform Surveillance (SUS) records are maintained under the following NARA citations: Electronic Products Reports- N1-088-08-1, Item 6.1, Exemption Requests and Variance Requests- N1-088-08-1, Item 6.2.1, Records with No Action- N1-088-08-1, Item 6.2.2.1, Records with Action- N1-088-08-1, Item 6.2.2.2, Inspection reports without problems- N1-088-08-1, Item 6.3.1, Inspection reports with problems- N1-088-08-1, Item 6.3.2, Certification Reports or Forms (e.g. FDA Form 2579)- N1-088-08-1, Item 6.4.2, X-Ray Assembler Certification Tracking Database Files- N1-088-08-1, Item 6.4.3, Laboratory Testing Records- N1-088-08-1, Item 6.5, Nation-wide Evaluation of X-Ray Trends(NEXT) Files- N1-088-08-1, Item 6.6. For all records pertaining to SUS, the disposition is temporary, and they are destroyed/deleted 10 years after the cutoff or when not required business use. Recall Records: Site inspection records; Device Registration and Listing data (DRLM) are maintained under the following NARA citation: N1-088-05-1, item 6.1 where the disposition is temporary, and the records transferred to the Federal Records Center (FRC) which is a backup system 5 years after cutoff date and then destroyed 10 years after the cutoff date. Radiological Health reviews (pre- and post-market) are maintained under NARA citation N1-088-08-1, Item 6.1 For these records, the disposition is temporary, and the records are destroyed or deleted 10 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.	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 the National Institute of Standards and Technology's (NIST's) Special Publication 800-53.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	7/16/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	7/16/2025
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:**	7/17/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 7/17/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	7/17/2025
SAOP Review Comments:	7/17/2025 Approved on behalf of the SAOP.	**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/17/2025 1:43 PM	BLAND, CRYSTAL	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	7/17/2025	7/17/2025 Per FDa's Email: • The PIA is experiencing an Archer error with question General 03: “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” o The FDA instance of Archer is automatically entering the answer “No,” which is incorrect. The ATO date is *1/23/2023*. o At this time, we are unable to update Archer to reflect the correct answer “Yes.” The FDA Archer Team is aware of this occurrence and is working on a solution.	CDRH Center Ad-hoc Reporting System_SOP approved.pdf 7-17-2025 EMAIL_PIA in Queue (CDRH Center Ad hoc Reporting System).pdf