Privacy Impact Assessment (PIA): FDA - CARS - QTR1 - 2022 - FDA2034778

Date Signed: 7/11/2022

**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

| | | | |
|---|---|---|---|
| **Status:** | Approved | **PIA ID:** | 1438441 |
| **PIA Name:** | FDA - CARS - QTR1 - 2022 - FDA2034778 | **Title:** | FDA - CDRH Reporting and Collection Tools |
| **OpDIV:** | FDA | | |

## PTA

| | | |
|---|---|---|
| **PTA - 1A:** | Identify the Enterprise Performance Lifecycle Phase of the system | Operations and Maintenance |
| **PTA - 1B:** | Is this a FISMA-Reportable system? | No |
| **PTA - 2:** | Does the system include a website or online application? | No |
| **PTA - 3:** | Is the system or electronic collection, agency or contractor operated? | Agency |
| **PTA - 3A:** | Is the data contained in the system owned by the agency or contractor? | Agency |
| **PTA - 5:** | Does the system have or is it covered by a Security Authorization to Operate (ATO)? | Yes |
| **PTA - 5A:** | If yes, Date of Authorization | 3/15/2022 |
| **PTA - 6:** | Indicate the following reason(s) for this PTA. Choose from the following options. | PIA Validation (PIA Refresh) |
| **PTA - 7:** | Describe in further detail any changes to the system that have occurred since the last PIA | CARS was recently updated: |

| | | |
|---|---|---|
| | | 1. To replace the CTRS system with the Insight Time Reporting System (ITR) which is a Cloud based Salesforce application. Data from this system provides the same Timesheet data for FDA Employees that CTRS provided.<br>2. To replace the Primo/SUS systems with eMDR data for Post Market Surveillance. Data provide by this system is the same data that was provided by Primo/SUS systems. |
| **PTA - 8:** | 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 Devices and Radiological Health (CDRH) and the Office of Regulatory Affairs (ORA) personnel (FDA employees and Direct Contractors), require access to the data in the 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.<br>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, 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.<br>CDRH and ORA 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 Food and Drug Administration (FDA) systems.<br>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 - 9:** | 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. | 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.<br>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.<br>CDRH and ORA personnel (permanent employees and Direct Contractors) do not use personal identifiers to retrieve data from CARS data warehouse. |
| **PTA -9A:** | Are user credentials used to access the system? | No |

| | | |
|---|---|---|
| **PTA - 10:** | 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 | CDRH and ORA 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.<br>The CDRH Ad-Hoc Reporting system, also known as the CARS data warehouse, imports data from the following internal FDA systems: 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 ORA'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).<br>These internal FDA source systems, briefly described below, are addressed in separate Privacy Impact Assessments (PIAs).<br>A single CARS Data Warehouse is maintained by CDRH. CDRH and ORA management grants users' access to specific data based on individual user role/duties and their need-to-know. CDRH and ORA 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.<br>For further information regarding the components of CDRH Center Ad-hoc Reporting System or CARS, please see the attached PIA dated, 2-28-2022. |
| **PTA - 10A:** | Are records in the system retrieved by one or more PII data elements? | No |
| **PTA - 11:** | Does the system collect, maintain, use or share PII? | Yes |

## PIA

| | | |
|---|---|---|
| **PIA - 1:** | Indicate the type of PII that the system will collect or maintain | Name<br>E-Mail Address<br>Phone numbers<br>Date of Birth<br>Mailing Address<br>Devices Identifiers<br>Others - 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 - 2:** | Indicate the categories of individuals about whom PII is collected, maintained or shared | Business Partners/Contacts (Federal, state, local agencies)<br>Employees/ HHS Direct Contractors<br>Patients |
| **PIA - 4:** | For what primary purpose is the PII used? | Center for Devices and Radiological Health (CDRH) and Office of Regulatory Personnel (ORA) 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 companies' providing submissions. |
| **PIA - 7:** | 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 - 9:** | Identify the sources of PII in the system | Directly from an individual about whom the information pertains<br>Online<br>Government Sources<br>Within the OPDIV |
| **PIA - 10:** | Is the PII shared with other organizations outside the system's Operating Division? | No |
| **PIA - 11:** | Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason | 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.<br>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.<br>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.<br>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.<br>This Privacy Impact Assessment provides further notice. |
| **PIA - 12:** | Is the submission of PII by individuals voluntary or mandatory? | Voluntary |
| **PIA - 13:** | Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason | There is no opt out process specific to the CARS system. Any PII in CARS is collected by the source system and any opt-out process would be provided by those systems. In this case, CDRH and ORA personnel including Direct Contractors cannot opt out regarding the collection of their PII. Submitters provide their contact information as a practical requirement in order to communicate with the FDA about submissions.<br>CDRH and ORA personnel (permanent employees and Direct Contractors) and customer contact PII is required to contact or generate correspondence that is sent to customers.<br>Collection of the information about external individuals from other FDA systems (e.g., industry submits points of contact and adverse event submitters). |
| **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 | 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 - 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 | 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).<br>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 Systems Management Center (SMC) and other agency offices, via email, phone and standard mail avenues (all listed on fda.gov and the FDA intranet).<br>In the event of a suspected incident or data breach, FDA personnel must report that without delay to the FDA's Systems Management Center (SMC) |
| **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 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 - 17:** | Identify who will have access to the PII in the system and the reason why they require access | Users<br>Administrators<br>Developers<br>Contractors |
| **PIA - 17A:** | Provide the reason of access for each of the groups identified in PIA -17 | |

| | | |
|---|---|---|
| | Users: For data analysis and reporting purposes. Some users are Direct Contractors.<br>Administrators: Require access for system maintenance and administrative purposes. Some administrators are Direct Contractors.<br>Developers: For development and support purposes. Some of the developers are Direct Contractors.<br>Contractors: Direct contractors that provide development, support, maintenance, and data analysis. | |
| **PIA - 17B:** | Select the type of contractor | HHS/OpDiv Direct Contractor |
| **PIA - 18:** | 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 - 19:** | 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 | CDRH and ORA 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.<br>Access to CDRH Time Reporting System (CTRS) in CARS is restricted to FDA employees only. An FDA Employee who has administrator privileges manages this database. |
| **PIA - 20:** | Identify training and awareness provided to personnel (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 Information Management and Technology (OIMT) verifies that training has been successfully completed by FDA employees and Direct Contractors. |
| **PIA - 23:** | Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific 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 N1-088-081 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 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 N1-88-07-2. For these records, the disposition is temporary, and the records are destroyed or deleted 10 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.<br>Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools.<br>Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls.<br>Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53. |