Privacy Impact Assessment (PIA): FDA - CDM - QTR4 - 2024 - FDA4563418

Created Date: 10/22/2024 4:26 PM Last Updated: 11/13/2024 1:20 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 - CDM - QTR4 - 2024 - FDA4563418 | **PIA ID:** | 2350971 |
| **Name of Component:** | FDA - OC Continuous Diagnostics Monitoring | **Name of ATO Boundary:** | OC GSS4 Enterprise Tools and Services |
| **Overall Status:** |  | **PIA Queue:** | |
| **Submitter:** | | **# Days Open:** | 22 |
| **Submission Status:** | Submitted | **Submit Date:** | 10/22/2024 |
| **Next Assessment Date:** | N/A | **Expiration Date:** | 1/1/2100 |
| **Office:** | | **OPDIV:** | FDA |
| **Security Categorization:** | | **OpDiv PIA ID:** | FDA4563418 |
| **Legacy PIA ID:** | | **Make PIA available to Public?:** | Yes |

| | | |
|---|---|---|
| **1:** | Identify the Enterprise Performance Lifecycle Phase of the system. | Operations and Maintenance |
| **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. | 10/12/2022 |
| **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 Food and Drug Administration (FDA) Office of the Commissioner (OC) Continuous Diagnostics and Mitigation (CDM) system was developed to improve the Agency's cybersecurity posture and meet current federal cybersecurity requirements. OC CDM uses automated continuous monitoring sensors to scan for and detect cyber threats and weaknesses within FDA information technology (IT) systems and networks. System functionality includes services to implement sensors and dashboards; delivery of near-real time results; priority categorization of incidents within minutes; the identification and mitigation of system flaws at network speed; and the ability to lower operational risk and exploitation of government IT systems and networks.<br><br>OC CDM include the following tools and functionalities: (a) ForeScout - Hardware Asset Management (HWAM); (b) Big Fix- Software Asset Management (SWAM); Configuration Management (CM); and Vulnerability Management (VUL); (c) Splunk – Data ingestion into CDM; and (d) Credential Management (CREDMGMT) – Access credential management and authentication solution that implements SailPoint to create a Master User Record (MUR). The MUR serves as a repository for user-related data that is collected from OC CDM. Additionally, the MUR addresses authentication privileges for nonprivileged users on the network; and improves the identity/access management of user's accounts. Through automated tools and dashboard integration, OC CDM allows FDA to run reports and create metrics to understand what and who is on the agency network.<br><br>OC CDM users include FDA permanent employees and Direct Contractors. |

| | | |
|---|---|---|
| **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. | OC CDM collects and maintains personally identifiable information (PII). PII data is collected via an interconnection with FDA's Active Directory (AD) and the Enterprise Administrative Support Environment (EASE) system (accessed separately). The OC CDM CREDMGMT tool collects and stores the following PII from users (FDA permanent employees and Direct Contractors): (a) first and last name; (b) Social Security number (SSN); (c) e-mail address; (d) phone number; (e) date of birth (DOB); (f) mailing address; (g) education records; (h) military status; (i) foreign activities; and (j) employment status. CREDMGMT retains PII data for an indefinite period of time. The PII data pulled from AD/EASE refreshes every 24 hours, and if a record is removed from the source, then it is also removed from the Sailpoint MUR. CREDMGMT does not collect any non-PII data. Users of CREDMGMT can use any of the PII elements that are collected by CREDMGMT to retrieve records held within the system.<br><br>BigFix and ForeScout tools identifies endpoints (i.e. Server, workstation, switch, router) by Internet Protocol (IP) addresses and only collects configuration data, such as endpoint name, Operating System (OS) data, installed software, Hard Drive (HD) space, and patch data. BigFix and ForeScout do not collect or store any PII. All data collected and maintained by BigFix and ForeScout is non-PII.<br><br>Splunk collects log data from configuration logs, security logs, network logs, and change logs. Splunk collects the following PII via logs: first name, last name, username, and email address.<br><br>PII data is only shared with the Department of Health and Human Services (HHS). HHS passes the shared data to the Department of Homeland Security (DHS). Data that is shared with HHS is sent in the form of logs via Splunk for the purpose of cybersecurity risk posture analysis. This data is used by the DHS for cross government identity management. Data that is sent from HHS to DHS does include PII. |
| **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. | OC CDM provides capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. FDA-installed sensors are deployed and perform an on-going, automated search for known cyber flaws. Results from the sensors feed into an FDA dashboard that produces customized reports that alert network managers to their most critical cyber risks. Prioritized alerts |

| | | |
|---|---|---|
| | | enable FDA to efficiently allocate resources based on the severity of the risk. Results are tracked through progress reports, which can be used to compare security postures among FDA networks. Cybersecurity risk posture across the Federal Government can be determined through summary information which feeds into a federal enterprise-level dashboard.<br><br>OC CDM tools include: (a) ForeScout – for management and control of devices (hardware asset management); (b) BigFix – for management and control of software (Software Asset Management); security configuration settings (Configuration Settings Management), and vulnerability management; (c) Splunk – Ingests, categorizes, and aggregates machine (event log) data in a secure, searchable repository and provides actionable data in the form of graphs, reports, alerts, dashboards, and visualizations to be used for cybersecurity operations and compliance use-cases while reducing Cyber Security and business risks; and (d) CREDMGMT-The CREDMGMT solution implements SailPoint which creates a Master User Record (MUR) which serves as a repository for user-related data that is collected from CDM tools and sensors. SailPoint enables collectors to capture data elements or attributes for specific security controls and enforces the appropriate usage of participating agency credentials and privileged accounts. SailPoint logs are ingested into Splunk. The MUR ensures strong authentication for non-privileged users on the FDA network, tightens policies and practices for network users, and improves the identity and access management of user accounts on federal information systems. The MUR collects and stores PII, which is used for correlation between the systems to connect the identity stored in different data sources for identity unification.<br><br>CREDMGMT collects PII because this tool is connected with Active Directory (AD) and Enterprise Administrative Support Environment (EASE). From AD/EASE, CREDMGMT collects the following PII data: name, social security number (SSN), e-mail address, phone number, date of birth (DOB), mailing address, education records, military status, foreign activities, and employment status. Users of CREDMGMT retrieve records held within the system using PII about personnel.<br><br>PII data is only shared with Health and Human Services (HHS). HHS passes the shared data to the Department of Homeland Security (DHS). Data that is shared with HHS is sent in the form of logs via Splunk for the purpose of cybersecurity risk posture analysis. This data is used by the DHS for cross government identity management. Data that is sent from HHS to DHS does include PII. |
| **PTA - 7:** | Does the system collect, maintain, use or share PII? | Yes |

| | | |
|---|---|---|
| **PTA - 7A:** | Does this include Sensitive PII as defined by HHS? | Yes |
| **PTA - 8:** | Does the system include a website or online application? | No |
| **PTA - 8A:** | Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)? | |
| **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. | |
| **PTA - 10:** | Does the website have a posted privacy notice? | |
| **PTA - 11:** | Does the website contain links to non-federal government websites external to HHS? | |
| **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? | |
| **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? | |
| **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. | Social Security Number<br>Name<br>Email Address<br>Education Records<br>Military Status<br>Foreign Activities<br>Date of Birth<br>Mailing Address<br>Employment Status |
| **PIA - 2:** | Indicate the categories of individuals about whom PII is collected, maintained or shared. | Employees/ HHS Direct Contractors |
| **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? | For CREDMGMT, the primary purpose that PII is used (within the MUR) for identity and credential management. PII is used for correlation between the systems to connect the identity stored in different data sources for identity unification. FDA sharing of PII in this system is limited to sharing with HHS. Once received by HHS, HHS assumes responsibility for data security and governance. HHS sharing includes providing data to DHS for Cross Government Identity Management. |
| **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. | The SSN is used for identity and credential management. |
| **PIA - 6A:** | Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. | For EASE the legal authority to use SSN is supported by Executive Order 9397, as amended, and CREDMGMT relies on EASE data.<br><br>DHS has mandated FDA to implement CREDMGMT solution as per Executive Order 13636 and 13800. |
| **PIA - 7:** | Identify legal authorities governing information use and disclosure specific to the system and program. | CREDMGMT sources its data from FDA EASE and FDA AD. The legal authorities governing information use and disclosure specific to the source systems are as follows: 5 United States Code (U.S.C) 301; 5 U.S.C. Sec. 3101; Homeland Security Presidential Directive (HSPD) 12; Executive Order 9397, as amended. |
| **PIA - 8:** | Are records in the system retrieved by one or more PII data elements? | Yes |
| **PIA - 8A:** | Please specify which PII data elements are used to retrieve records. | Depending on their work needs, users of CREDMGMT use different PII elements to retrieve records. They are able to use name, Social Security number, e-mail address, phone number, date of birth, mailing address, education records, military status, foreign activities, and employment status. |

| | | |
|---|---|---|
| **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. | 1) SORN 09-90-0777, Facility and Resource Access Control Records;<br><br>2) SORN OPM GOVT-1, General Personnel Records |
| **PIA - 9:** | Identify the sources of PII in the system. | Directly from an individual about whom the information pertains<br><br>Online<br><br>Government Sources<br><br>Within the OPDIV |
| **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. | N/A. The system does not collect any information from members of the public. |
| **PIA - 11:** | Is the PII shared with other organizations outside the system's Operating Division? | Yes |
| **PIA - 11A:** | Identify with whom the PII is shared or disclosed. | Within HHS |
| **PIA - 11B:** | Please provide the purpose(s) for the disclosures described in PIA - 11A. | Credential Management and Identity Unification. |
| **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)). | DHS Mandate for Credential Management. An Information Sharing Agreement (ISA) is currently being executed between HHS and FDA. |
| **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. | FDA does not disclose records from this system outside HHS. Disclosures made within HHS are for authorized need-to-know purposes. The Privacy Act does not require an accounting of such disclosures within HHS. To the extent HHS discloses records outside of HHS, the disclosing HHS office is responsible for maintaining an accounting.<br><br>In the event FDA discloses records outside HHS and the disclosures require an accounting the system manager will maintain an accounting. The FDA Privacy Office provides guidance on the specific elements of the disclosure accounting.<br><br>FDA also adheres to logging and event aggregation requirements of the Federal Information Security Modernization Act (FISMA). |
| **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. | Employment at FDA is voluntary, however the provision of PII is necessary to perform job duties. Individuals cannot opt out and continue to meet their employment obligations. The information is required to appropriately clear employees and contractors, award them appropriate access, and conduct necessary functions such as tracking the provision of mandatory training, tracking computers and other equipment assigned, issuing PIV badges, and others. |
| **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 that would affect the rights or interests of the individuals are anticipated. However, if FDA 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 an FDA web site, e-mail notice to the individuals, inclusion in newsletters, or information provided to supervisors with instructions to further inform staff. |
| **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 will be a SailPoint Queue (reporting/assistance line) in the helpdesk ticketing system to address any individual user concerns as they arise.<br><br>In the event any employee suspects his or her information has been compromised, inappropriately accessed or used, or is incomplete, incorrect, or out-of-date, the individual can contact the Employee Resource and Information Center (ERIC) and request assistance; contact the FDA Privacy Office directly; contact supervisors, managers, and team leaders; and/or report potential loss or misuse of their PII to FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC).<br><br>All system users are required to immediately report suspected incidents and breaches. |
| **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. | The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Integrity and availability are protected by security controls selected and implemented in the course of providing the system with an authority to operate (ATO). Information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information are in place. Data discrepancies identified in the course of system use are addressed when discovered. Controls are selected based on National Institute of Standards and Technology (NIST) guidance. |

| | | |
|---|---|---|
| **PIA - 17:** | Identify who will have access to the PII in the system. | Administrators<br>Developers<br>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. | Administrators: Management and updating of the system. Some of the administrators are Direct Contractors.<br>Developers: Development of reports and configurations relating to gathering of such information<br>Contractors: Direct Contractors that will be providing administrative support for the system. |
| **PIA - 19:** | Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII. | Role Based Access Control (RBAC) is applied when creating user accounts to the system. Accounts created via RBAC are utilized for requesting and obtaining approval to access PII data. Only users with a need-to-know are granted access to PII. Approval is granted by the System Owner and access is audited. |
| **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. | The concept of 'least privilege' and 'need-to-know' have been applied in the account management process. Role based access (RBAC) with applied technical controls is employed to ensure that users have only the necessary access to perform their job duties. |
| **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 Information Management and Technology (OIMT) verifies that training has been successfully completed and maintains a record of certificates of training on all FDA employees and direct contractors. Additionally, HHS will provide tool specific training on BigFix, ForeScout, Splunk, and SailPoint (CREDMGMT). |
| **PIA - 22:** | Describe the training system users receive (above and beyond general security and privacy awareness training). | There is no further training for general users beyond the general security and privacy training at the FDA. Individuals with significant security responsibilities must complete additional security and privacy training annually. Additional training is available from the FDA 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). | CREDMGMT obtains PII from EASE, a separate FDA system. Records are maintained by a schedule in the FDA 9110 File Code series, specific to EASE, including File Codes 9111 through 9117 inclusive. 9111 covers Inputs (Core and Other Data), which is to say, data that may be updated by newer information provided by the Enterprise Human Resources and Payroll System (EHRP) system, at which time the previous data may be overwritten and destroyed.<br><br>All other applications in this are maintained under General Records Schedule (GRS) 3.2, Information Systems Security Records; Item 030, System Access Records. This schedule is for "records created as part of the user identification and authorization process to gain access to systems." Disposition for these files is temporary, and the files may be destroyed/deleted when business use ceases. If the application owner determines that an application requires special accountability, retention may be six years after the password is altered or the user account is terminated, and longer retention is authorized if required for business use. |
| **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 NIST's Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199. |

## Review & Comments

### Privacy Analyst Review

| | | | |
|---|---|---|---|
| **OpDiv Privacy Analyst Review Status:** | Approved | **Privacy Analyst Review Date:** | 10/22/2024 |
| **Privacy Analyst Comments:** | | **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. | **SOP Review Date:** | 10/22/2024 |
| | | **SOP Days Open:** | 0 |

### Agency Privacy Analyst Review

| | | | |
|---|---|---|---|
| **Agency Privacy Analyst Review Status:** | Approved | **Agency Privacy Analyst Review Date:** | 10/24/2024 |
| **Agency Privacy Analyst Review Comments:** | Reviewer: Nestor Villafuerte<br><br>10/24/2024 This PIA is ready for SAOP review and approval. | **Agency Privacy Analyst Days Open:** | 2 |

### SAOP Review

| | | | |
|---|---|---|---|
| **SAOP Review Status:** | Approved | **SAOP Signature:** | Archer Signature_Bridget Guenther.docx |
| **SAOP Comments:** | The PIA is currently experiencing an Archer error with Question #3 of the general information.<br><br>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."<br><br>The FDA Archer Team is aware of this occurrence and is working on a solution. | **SAOP Review Date:** | 11/13/2024 |
| | | **SAOP Days Open:** | 20 |

### Supporting Document(s)

| Name | Size | Type | Upload Date | Downloads |
|---|---|---|---|---|
| 10-23-2024 Email_PIA in Queue (OC Continuous Diagnostics Monitoring).pdf | 285778 | .pdf | 10/23/2024 9:56 AM | 0 |
| OC Continuous Diagnostics Monitoring_SOP Approved.rtf | 764024 | .rtf | 10/23/2024 9:56 AM | 0 |

## Comments

| Question Name | Submitter | Date | Comment | Attachment |
|---|---|---|---|---|
| PIA - 1 | BLAND, CRYSTAL | 10/23/2024 | Per FDA 's Email:<br><br>The PIA is currently experiencing an Archer error with Question #3 of the general information.<br><br>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.”<br><br>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:** | 11/13/2024 1:20 PM | **History Log:** | View History Log |