Privacy Impact Assessment (PIA): FDA - APM - QTR3 - 2024 - FDA3724782

Created Date: 9/25/2024 8:24 AM Last Updated: 10/3/2024 4:27 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 - APM - QTR3 - 2024 - FDA3724782	**PIA ID:**	2250700
Name of Component:	FDA - OC AppDynamics Enterprise Application Performance Monitoring	**Name of ATO Boundary:**	OC GSS4 Enterprise Tools and Services
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	16
Submission Status:	Submitted	**Submit Date:**	9/24/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA3724782
Legacy PIA ID:		**Make PIA available to Public?:**	No

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)?	Yes
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.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	No changes to PTA/PIA status since original review
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) Application Performance Monitoring (APM) tool is a Commercial off the Shelf (COTS) product FDA purchased from Cisco/AppDynamics. As one component of the Agency's General Support System 4 (GSS 4), the purpose of the OC APM) tool is to provide insight into application performance and usage for the FDA Application Suite. OC APM provides a user interface that has dashboards showing real-time performance metrics for each monitored FDA application, as well as across multiple applications. Resources monitored includes business transaction performance, along with underlying infrastructure metrics. The tool is available for FDA Center Developer/Application teams to monitor the performance of their applications, and to debug and perform root cause analysis when issues occur. The tool is only available to internal FDA teams and is not accessible to the public in general.

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 APM collects limited personally identifiable information (PII) consisting only of usernames, work email addresses and possibly names for FDA permanent employees and Direct Contractors. This is NOT used for the login process for APM/AppDynamics (which is offloaded to FDA single sign-on (SSO) using Personal Identification Verification (PIV) card authentication). This data is captured incidentally from applications that make it available in their headers or sessions and is not directly requested or gathered by the APM tool. This data is observed by the monitoring tool, but originally gathered by the monitored applications. OC APM collects non-PII data associated specifically with low-level server and application infrastructure metrics, such as application/server response times, error rates, error messages, Central Processing Unit (CPU) load, random-access memory (RAM) usage, and Heap Usage. These metrics are not specific to users of the tool. AppDynamics also monitors the business transactions for each application, and in doing so captures header and session information for that application's business transaction. Depending on their implementation, the applications may have username, user email information and name in their sessions and headers due to their use of FDA Single Sign-On (SSO). OC APM may capture this information in metric snapshots. This stored transaction data is used by application teams to debug performance and functional issues when they occur. No passwords from the monitored applications are captured. No FDA PIV card certificates, credentials, or other information is captured or stored in OC APM. The capturing and storing of the PIV card information used for access control and SSO is offloaded to the FDA Oracle Access Manager (OAM) SSO system.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card

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 APM enables FDA to monitor application performance and address performance problems. The effective use of the OC APM tool requires collection of certain technical metrics as well as limited PII typically captured incidental to system functionality. Users of OC APM consist of FDA permanent employees who are a part of the FDA Center Application teams. Some of the users are also Direct Contractors. Specifically, users consist of Administrators (FDA permanent employees and APM Direct Contractor Team) and Application Developers (FDA permanent employees and Direct Contractors). All users log in using FDA SSO. PIV credentials are not stored in the OC APM system. The OC APM tool does not request PII from individuals, nor disclose the basic user login information (usernames, email addresses). Rather, it inherits it second hand from the sessions/headers of the instrumented applications. That is, the PII data is originally gathered by the monitored application, and not APM. This data is purely used for application performance analysis and debugging. Members of the public do not have access to FDA OC APM and AppDynamics. Access is controlled within secure firewalls by PIV authenticated FDA SSO. The OC APM console users are FDA Center Application Teams. Application Team users are only granted access to their specific application dashboards using role-based access. Therefore, they are only able to view the data that came originally from their system(s). Hence, any PII gathered by the APM system is only shared with the original app teams that collected that PII from users in the first place. This PII is used for debugging of application performance issues. FDA Application Teams who access or use the OC APM system do not use any PII to retrieve records held in the system.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	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.	Name Email Address User Credentials
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.	201 - 500

PIA - 4:	For what primary purpose is the PII used?	The session and header information gathered automatically from the monitored applications that may include the incidental collection of PII (FDA usernames, FDA email addresses and names of FDA personnel and Direct Contractors) is used by application teams to debug application performance issues when they occur. For instance, if a specific report generation caused a system crash, they may be able determine the user that performed the action to get more details from them, and further the root cause analysis.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Some Application teams may use the username and/or email addresses, where available, to perform basic analytics for statistics about users logging in to their applications, user volume and similar application performance and use data. The information is never used outside of the FDA. This information is only available to the team that specifically owns each application.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 U.S.C. 301.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	
PIA - 9:	Identify the sources of PII in the system.	Government Sources 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.	OC AppDynamics Enterprise Application Performance Monitoring does not collect any information on the public and does not require an OMB information collection approval number.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary

PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	OC APM is a monitoring system, and merely observes some basic user info for users logging in to a subset of the instrumented applications. It does not directly request or require PII from users, but rather sees information in the sessions of the instrumented FDA applications. There is no opt-out process specific to APM use. The limited PII involved is necessary for the use of the tool and the effective resolution of application performance issues.
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.	The monitored FDA Applications collecting the original PII data that OC APM observes will employ procedures to notify and obtain consent from their users when major changes occur to their systems. Should OC APM use ever change such that individuals should be notified of OC APM use or disclosure of their PII, FDA will use the most effective means to provide this notice to affected users, such as email, display of notice within the UI or similar methods.
PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Individuals who suspect their PII has been inappropriately obtained, used or disclosed in an FDA system have a number of methods available to correct the situation. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource Information Center (ERIC), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and other agency offices via email, phone and postal mail (all of which are listed on FDA.gov and FDA intranet). In the event of a suspected incident or data breach, FDA personnel must report without delay to FDA's CIOCC.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	The FDA Applications collecting the PII data that the OC APM tool observes are responsible for periodic reviews of PII contained in their systems, to include data integrity, availability, accuracy, and relevancy. OC APM purely sees this data as the result of incidental capture.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Administrators- OC APM Administrators have access to view the metric data gathered by the APM agents on the instrumented applications. This metric data can include the limited PII (FDA Usernames, FDA email addresses) observed from the monitored FDA Applications. This is necessary to manage and maintain the OC APM monitoring infrastructure. Developers-FDA Application teams will have access to the metrics collected for their specific applications. This metric data can include the limited PII (FDA Usernames, FDA email addresses) observed from their monitored FDA Application. This is so that they can debug system performance issues and monitor their infrastructures. Some of the developers are Direct Contractors. Contractors-Some of the FDA Developers are Direct Contractors.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The OC APM system uses Role-Based Access Controls to control who has access to the data collected by the system from the various applications. The OC APM Administrator Team has access to all applications by default, as is required to be able to manage and deploy the application monitoring. OC APM Administrators are approved for this access by the FDA OC APM Management Team. FDA Application Team Program Managers and Leads provide the requested access lists for each specific application that is monitored by AppDynamics. Therefore, any user with access to the application data in the AppDynamics has been explicitly approved to have that access by the FDA management team for that Center or Application.
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 OC APM system uses Role-Based Access Controls, supported by technical measures (e.g., SSO) to ensure that Application Teams with AppDynamics console access can only see data for their specific applications. This means that any PII is only accessible to the Application Team that originally collected that data in their system.
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 FDA permanent employees and Direct Contractors take FDA mandatory Privacy, Security and Records Management training at least once a year.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	OC APM Administrators are required to take all the mandated FDA training for privileged account holders. Training sessions on using the APM Console are provided by the APM team to Application Teams on request.

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).	The General Records Schedule (GRS) 3.2-Information Security Records, Item 031-System Access Records is used to manage the disposition of the records this system creates. The disposition is temporary. The records are destroyed 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. This is done under disposition authority DAA-GRS-2013-0006-0004.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (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:**	9/25/2024
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:**	9/25/2024
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	9/26/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 9/26/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	10/3/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
9-24-2024 FDA EMAIL PIA In Queue (OC AppDynamics Enterprise Application Performance Monitoring).pdf	303510	.pdf	9/25/2024 9:53 AM	1
OC AppDynamics Enterprise Application Performance Monitoring_SOP Approved.pdf	167158	.pdf	9/25/2024 9:52 AM	1

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	9/26/2024	Per FDA Email (see Supporting Documentation): This PIA is currently experiencing an Archer error with Question #3 of the general information. Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)? The FDA instance of Archer is reflecting “No” as the answer when the correct answer is “Yes.”	

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:	10/3/2024 4:27 PM	**History Log:**	View History Log