Privacy Impact Assessment (PIA): FDA - MDSAP - QTR3 - 2023 - FDA2107889

Created Date: 8/30/2023 4:02 PM Last Updated: 3/7/2024 1:03 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 - MDSAP - QTR3 - 2023 - FDA2107889	**PIA ID:**	1699403
Name of Component:	FDA - CDRH Medical Device Single Audit Program Regulatory Exchange Platform-secure	**Name of ATO Boundary:**	CDRH Reporting and Collection Tools
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	218
Submission Status:	Submitted	**Submit Date:**	1/29/2024
Next Assessment Date:	N/A	**Expiration Date:**	3/7/2027
Office:		**OPDIV:**	FDA
Security Categorization:	Moderate	**OpDiv PIA ID:**	FDA2107889
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)?	Yes
4:	ATO Date or Planned ATO Date.	1/23/2023
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 Medical Device Single Audit Program Regulatory Exchange Platform (MDSAP) is a component under CDRHs Reporting and Collection Tools system and supports a group of international members as a joint, global IT portal. MDSAP was part of the PAHO Regulatory Exchange Platform - secure (REPs) platform that was a web-based data hub for efficient and dynamic information sharing among worldwide groups with varying use permissions. The participating users include National Regulatory Authorities (NRA) and other select auditing organizations (AO) (e.g., third-party auditors). MDSAP is an international regulatory audit program designed to allow medical device manufacturers to undergo a single audit to meet the quality management system requirements of multiple regulatory authorities. The program was developed by the International Medical Device Regulators Forum (IMDRF) to streamline the regulatory audit process and reduce regulatory burden on manufacturers. Under the MDSAP, a single audit can be conducted by an authorized auditing organization to assess a manufacturer's compliance with the quality management system requirements of participating regulatory authorities, including the U.S. Food and Drug Administration (FDA), Health Canada, the Australian Therapeutic Goods Administration (TGA), the Japanese Pharmaceuticals and Medical Devices Agency (PMDA), and the Brazilian Agência Nacional de Vigilância Sanitária (ANVISA).
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.	MDSAP contains the following types of information: Confidential/non-public information (NPI) from outside organizations including other governments as well as approved auditing organizations (in MDSAP case: Audit Package Documents: Audit Plans, Audit Reports, NGEs, and Product Lists); Names, email addresses, CVs, training certificates Client/Facility information submitted by outside organizations. Stored information is retained indefinitely.
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 HHS Username Password Non-HHS User Credentials Password

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.	Information about users is maintained in order to facilitate ongoing contact between them and the FDA.
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?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes
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.	Regulatory Exchange Platform – secure (REPs) MDSAP provides a collaborative platform for auditing organizations and regulatory authorities to manage audit reports, policies and procedures, and facility profiles. Auditing organizations and regulatory authorities have access to the website which is accessed via the public URL.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 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?	No
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?	No
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 Phone numbers User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Vendors/Suppliers/Third-Party Contractors (Contractors other than 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?	PII is collected to contact individuals at medical device manufacturing facilities.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	N/A
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.	N/A
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.	N/A
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.	N/A
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Other Federal Entities Non-Government Sources Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	0910-0886
PIA - 10B:	Identify the OMB information collection approval number expiration date.	4/30/2023

PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A
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.	Opt-out through non-participation in the program. Language to this effect is part of the Security Warning banner that is displayed upon accessing the application URL. A user must click "Accept" before being allowed to access the application.
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 changes are planned or anticipated. If such a change is made, individuals whose information is maintained in MDSAP will be notified via email along with updates to system documentation identifying the use of PII.
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.	Users are advised to contact the FDA MDSAP Help Desk. mdsap.support@fda.hhs.gov.
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.	No regular periodic review – regulatory audits are performed as needed. MDSAP audit report contents are controlled by the MDSAP program policies and procedures. They contain nonpublic information as well as PII.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Admins: Need to review/configure and report on requests made on PII. (Based on admin role, not all admins have access to PII.) User: Access restricted to user's own data. Developers: Access is only in lower environments, never to higher developers.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Zero Trust and Least Privilege is enabled for all users. Every additional access requires review and approval.
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.	Two factor authentication for all users Data encryption (at rest and in transit) for the system components (Advanced Encryption Standard (AES) 256 Key for at rest) (On govcloud not encryption for info in transit).
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.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	N/A
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).	For the contact information PII in the system, the current retention schedule is FDA File Code 7222, Database Records, National Archives and Records Administration (NARA) Approval N1-88-07-2. Retention is temporary, with cutoff after the establishment goes out of business or the product is no longer commercially marketed, and the records would be deleted or destroyed after ten years after cutoff or when no longer needed for legal, research, historical or reference purposes, whichever is the latest. System account credentials remain available as long as each user has authorized access to the system. Credentials are revoked when access is no longer needed, including if the individual moves to a different office within FDA or leaves FDA employment. These records are maintained under FDA File Code 9962 (NARA GRS 20, Item 1c; superseded by the new General Records Schedule (GRS) 3.2, item 030 (DAA-GRS-2013-0006-0003), which is for “records … created as part of the user identification and authorization process to gain access to systems. " Under this schedule, retention is until "business use ceases." In other words, NARA concurs that agencies may dispose of these records as soon as they are no longer needed.

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.	Two factor authentication for all users Zero Trust and Least Privilege is enabled for all users. Every additional access requires review and approval. Zero Trust is a security principle in which access to an environment does not depend in any way on the honesty of users, granting access only to those who've proven their identity and right to do so. Least Privilege is a security principle in which only the permissions needed to perform a role are granted, and absolutely no others. Data encryption (at rest and in transit) for the system components (AES 256 Key for At rest) (On govcloud not encryption for info in transit). Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	1/29/2024
Privacy Analyst Comments:	Updated PIA Reponses: PIA - 1, PIA-13, PIA-23, and PIA-24	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Responded to HHS questions.	**SOP Review Date:**	1/29/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	1/31/2024
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski Comments have been addressed in PIA-23. This PIA is ready for SAOP review and approval. Request SAOP review of the records retention response. 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:	In the next iteration, please update PTA 5 as it states: Stored information is retained indefinitely. This response does not match with records PIA question.	**SAOP Review Date:**	3/7/2024
		SAOP Days Open:	36

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
CDRH Medical Device Single Audit Program Regulatory Exchange Platform-secure_SOP Approved.pdf	236350	.pdf	8/31/2023 3:44 PM	0
CDRH Medical Device Single Audit Program Regulatory Exchange Platform-secure_SOP Approved_PIM_jl_v2.pdf	300141	.pdf	10/6/2023 8:30 AM	0
CDRH Medical Device Single Audit Program_SOP Approved.pdf	207799	.pdf	1/30/2024 9:14 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	LASKOWSKI, JAMES	8/31/2023	Per PTA-5A, user credentials are used to access the system. Please add user credentials to your response. Also, in the next iteration of the PTA, please spell out PAHO and NGEs on first use.	
PIA - 24	LASKOWSKI, JAMES	8/31/2023	Please describe the physical controls used by the system.	
PIA - 13	KORAN, ELIZABETH	10/24/2023	Please explain how individuals are made aware that their information will be collected so they can make this decision.	
PIA - 23	KORAN, ELIZABETH	10/24/2023	Please revise response to include the specific NARA schedule, include the schedule number, in addition to the retention periods. Please remove information about the internal functioning of the retention tool (e.g., (Close may need an extra rule on the folder if not automatically completed via this schedule see story PAHOREPS-STY-72 for details)) to avoid confusing the public.	
PIA - 23	LASKOWSKI, JAMES	1/30/2024	GRS 20 is obsolete and has been replaced by GRS 5.1 and 5.2	

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:	3/7/2024 1:03 PM	**History Log:**	View History Log