PTA / PIA: FDA - MedSun - QTR2 - 2025 - FDA4918547

Created Date: 4/23/2025 12:51 PM Last Updated: 4/25/2025 4:50 PM

General Information

PTA / PIA Name:	FDA - MedSun - QTR2 - 2025 - FDA4918547	**PTA / PIA ID:**	3073938
Component Name:	FDA - CDRH Medical Product Safety Network	**ATO Boundary Name:**	CDRH Reporting and Collection Tools
Overall Status:	Complete	**# of Days - Open:**	2
Submitter:		**Submit Date:**	4/23/2025
Next Assessment Date:	04/24/2028	**Expiration Date:**	4/24/2028
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	1/23/2023
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Jill Marion
PTA 01A:	POC Title and Organization	POC Title: MedSun Business Owner POC Organization: FDA/CDRH
PTA 01B:	POC Email Address	Jill.Marion@fda.hhs.gov
PTA 01C:	POC Phone Number	240-620-8133
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The Food and Drug Administration (FDA) has made no changes to this system/component since the last Privacy Threshold Analysis/Privacy Impact Assessment was approved.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	FDA Center for Devices and Radiological Health (CDRH) is responsible for protecting and promoting the public health. It assures that patients and providers have timely and continued access to safe, effective, and high-quality medical devices and safe radiation-emitting products. In keeping with its mission, CDRH launched, in 2002, an adverse event reporting program called the Medical Product Safety Network (MedSun). The program is an internet-based system under which healthcare facilities volunteer to submit reports of adverse events involving medical devices in their facility. The primary purpose of MedSun is to support collaboration with the clinical community to identify, understand, and solve problems associated with the use of medical devices.

PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	MedSun fosters an important partnership between clinical sites and FDA and serves as a powerful two-way channel of communication between CDRH and the clinical community. MedSun collects and maintains data concerning adverse events involving medical devices. Data processed in the system includes the device identifier or serial number, the reported event, as well as professional contact information about a person designated by the clinical facility (referred to in this assessment as reporter). MedSun only collects Personally Identifiable Information (PII) about reporters who are the designated point of contact (POC) from clinical facilities. PII collected includes name, work email address, work phone number, work mailing address, username, and password. Reporters access the MedSun internet portal using their username and password. This portal is not accessible by the general public; only specific and approved users/reporters are granted access to the website. MedSun does not collect, nor maintain any patient related information. FDA shares redacted and aggregated reports about a particular device and the associated health issues with the public. The system does not collect information about FDA employees or direct contractors. They access the system via a network-level single-sign-on process using multi-factor authentication (no username, password). MedSun does not maintain system-specific logon credentials (e.g., username and password) from FDA personnel. The retention and destruction process associated with the information contained within this system is continuously reviewed to ensure it complies with FDA and NARA regulations. The records in the database are destroyed 30 years after the database is closed.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Username Password

PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	MedSun enables an important collaborative partnership between clinical sites and FDA. Once a problem is identified, MedSun researchers work with each facility's representatives to clarify and understand the problem. Reports and lessons learned are shared with the clinical community and the public, without facility and patient identification, so that clinicians nationwide may take necessary preventive actions. The Safe Medical Devices Act (SMDA) defines 'user facilities' as hospitals, nursing homes, and outpatient treatment and diagnostic centers. They are required to report medical device problems that result in serious illness, injury, or death. MedSun participants are also highly encouraged to voluntarily report problems with devices, such as 'close-calls,' potential for harm, and other safety concerns. By monitoring reports about problems and concerns before a more serious event occurs, FDA, manufacturers, and clinicians work together proactively to prevent serious injuries and death. Participants use an Internet-based system that is designed to be an easy and secure way to report adverse medical device events. Each facility has online access to the reports they submit to MedSun so that they can be tracked and reviewed at any time. The general public cannot access the MedSun online portal as permission is only granted to individuals appointed by their facility. MedSun has two subnetworks. These subnetworks are designed to collect and share information about actual and potential adverse events from specific clinical areas of MedSun facilities using high-risk products. HeartNet: Focuses on identifying, understanding, and solving problems with medical devices used in electrophysiology laboratories. KidNet: Focuses on identifying, understanding, and solving problems with medical devices used in neonatal and pediatric intensive care units.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	Internal user url https://medsun-cdrh.fda.gov/ External users url https://medsun.fda.gov/
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes

PTA 09:	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.	The Medical Product Safety Network (MedSun) is an adverse event reporting program launched in 2002 by the U.S. Food and Drug Administration's Center for Devices and Radiological Health (CDRH). The primary goal for MedSun is to work collaboratively with the clinical community to identify, understand, and solve problems with the use of medical devices. MedSun fosters an important partnership between clinical sites and FDA. MedSun also serves as a powerful two-way channel of communication between CDRH and the clinical community. Once a problem is identified, MedSun researchers work with each facility's representatives to clarify and understand the problem. Reports and lessons learned are shared with the clinical community and the public, without facility and patient identification, so that clinicians nationwide may take necessary preventive actions. users access the web site via public URL, Login (username/password).
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 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Biographical Information Name User Credentials Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	50,000 – 99,999
PIA 25:	For what primary purpose is the PII used?	The PII, consisting of business contact information of facility points of contacts, is collected for communicating with facilities in relation to recall activities, and tracking and managing FDA's processing and administration of the activity.

PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	Username and password are maintained in MedSun in order to grant approved reporters' appropriate access to MedSun online portal.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	FDA uses this system to protect and promote the health and safety of the American public under the Federal Food, Drug and Cosmetic Act, 21 U.S.C. 301.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Non-Government Sources Members of the Public
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	OMB Information Collection Approval Number: 0910-0471 Expiration Date: 8/31/2026
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	While submission of PII is "voluntary" as that term is used in the Privacy Act, there is no option to opt-out. The PII is required in order to communicate with the facility points of contact in regard to product recall activities. The selection of the facility point of contact (POC) is at the discretion of the regulated industry, provided that person is the "Most Responsible Person" as indicated in the filing requirements.
PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	If there are major system changes impacting use of PII, FDA will assess the need to notify individuals and implement appropriate notice mechanisms such as e-mail or letters to facility contacts and/or posting notices online.
PIA 36:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Facility points of contact may submit concerns to their FDA liaison or other agency offices using the mailing addresses, email addresses and phone numbers available on FDA.gov, including FDA's privacy office.

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	Reporter's 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 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). 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 annual reviews to evaluate user access. One of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified in the course of system use are addressed when discovered.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: need access to PII is to process the information received from clinics and hospitals. Some users may include: supervisors, administrators, developers, and direct contractors. Administrators: Routine system Administration. Some administrators are Direct Contractors Developers: Developers perform system development data clean-up, and modifications as needed Contractors: Direct contractors are system administrators and developers.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	MedSun Application currently use the system assigned role to determine which user is allowed to access PII in MedSun. If the user has the required role assigned to them (i.e. Management or Admin) they will be allowed to access PII in MedSun.

PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Supervisors indicate on the account creation form the minimum information system access that is required in order for the user to complete his/her job. The access list for the information system is reviewed on a quarterly basis and users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All FDA users are trained on the system, and all users must annually complete FDA's information security and privacy awareness training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	FDA users receive system-specific training and may obtain additional privacy guidance from the agency's privacy officials. When joining the MedSun program, each designated reporter at a voluntarily participating facility is trained on the software.
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The retention and destruction process associated with the information contained within this system is continuously reviewed to ensure it complies with FDA and NARA regulations. The MedSun system received NARA approval September 24, 2002, Job number N1-088-02-01. Disposition: TEMPORARY: The records in the database are destroyed 30 years after the database is closed.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	4/23/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	4/23/2025
SOP Review Comments:	**The FDA's Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls.**	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	4/24/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 4/24/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	4/25/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	1

SAOP Signature

Date	User	Type	Name	Original Value	New Value
4/25/2025 1:43 PM	GUENTHER, BRIDGET	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	BLAND, CRYSTAL	4/24/2025	The PIA is experiencing an Archer error with question General 03: Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” • The FDA instance of Archer is automatically entering the answer “*No*,” which is incorrect. The ATO date is *1/23/2023*. • At this time, we are unable to update Archer to reflect the correct answer “Yes.” The FDA Archer Team is aware of this occurrence and is working on a solution.	PIA In Queue (CDRH Medical Product Safety Network) .pdf CDRH Medical Product Safety Network_SOP Approved_4.23.2025.pdf