


General Information		
<b>PTA / PIA Name:</b>	FDA - Qualtrics - QTR4 - 2025 - FDA5011883	<b>PTA / PIA ID:</b> 3971256
<b>Component Name:</b>	FDA - CDRH Qualtrics	<b>ATO Boundary Name:</b> CDRH Center Engagement and Workforce Development
<b>Overall Status:</b>	Complete 	<b># of Days - Open:</b> 34
<b>Submitter:</b>		<b>Submit Date:</b> 11/5/2025
<b>Next Assessment Date:</b>	N/A	<b>Expiration Date:</b> 1/1/2100
<b>Office:</b>		<b>OpDiv:</b> FDA
<b>Security Categorization:</b>	Low	
<b>Make PIA available to Public?:</b>	No	<b>PIA Required:</b> Yes
<b>General 01:</b>	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
<b>General 02:</b>	Is this a FISMA-Reportable system?	No
<b>General 03:</b>	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
<b>General 04:</b>	ATO Date or Planned ATO Date.	12/31/2025
<b>General 05:</b>	Is the system or electronic information collection, agency or contractor operated?	Contractor
<b>History Log:</b>	<a href="#">View History Log</a>	

Privacy Threshold Analysis		
<b>Privacy Threshold Analysis</b>		
<b>PTA 01:</b>	Point of Contact (POC) Name	Cathy Oliveri
<b>PTA 01A:</b>	POC Title and Organization	System Owner FDA/CDRH
<b>PTA 01B:</b>	POC Email Address	cathy.oliveri@fda.hhs.gov
<b>PTA 01C:</b>	POC Phone Number	301-796-5549
<b>PTA 02:</b>	Indicate the following reason(s) for this PTA. Choose from the following options.	New
<b>PTA 03:</b>	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.

Center for Devices and Radiological Health (CDRH) Qualtrics is an external-facing application that is hosted in a Federal Risk and Authorization Management Program (FedRAMP) authorized Software as a Service (SaaS) on the Qualtrics XM Platform. The system is used by United States Food and Drug (FDA)'s Medical Device Program to collect input from internal and external customers through surveys, which are distributed and managed using the Qualtrics SaaS platform. The system records, stores, and analyzes the results of this input, which is collected in an anonymous manner.

Key functionalities and features:

Collects anonymous survey responses from internal and external customers; records, stores, and analyzes the results of input collected; allows authorized end users to create, change, or delete published surveys; and manages access to surveys through user roles and permissions, distinguishing between administrators and standard users.

CDRH Qualtrics users consists of CDRH Qualtrics Administrators who have extensive control over the platform, and public users who primarily access anonymous surveys to respond to them. CDRH Qualtrics will be configured for CDRH Qualtrics Administrators to use multi-factor authentication (MFA) via Security Assertion Markup Language (SAML) / Single Sign-On (SSO) for authentication. Public users access anonymous surveys via survey links. No authentication is required for anonymous surveys.

<b>PTA 05:</b>	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.	<p>CDRH collects anonymous survey responses from internal and external customers.</p> <p>CDRH Qualtrics allows FDA to manage a survey as a service operation for the Center for Devices and Radiological Health (CDRH) enabling CDRH to collect information related to customer service both internally and externally. CDRH collects information related to customer satisfaction levels stakeholders both inside FDA/CDRH and external, including the medical device industry, academia, patient groups, health professionals, consumers and anyone that interacts with CDRH. These voluntary satisfaction surveys are anonymous and there is no collection of information to categorize survey respondents.</p> <p>The surveys gather information that allow customers to provide feedback about the quality of services provided. These answers are typically mostly numeric responses in a Likert Scale (e.g. rank from 1 to 5). Some survey questions allow users to select a response from a dropdown to identify the Center that provided the service.</p> <p>Some questions allow free response text. Free response text boxes allow the optional entry of the Name of an FDA employee or Direct Contractor. The Respondent provided PII (name of FDA Employee/Direct Contractor) is redacted after being converted to Organizational Identifiers. The free response text is screened for sensitive personally identifiable information (PII). If sensitive information is provided, there are security safeguards turned on to block transmission and prevent incidental capture.</p> <p>FDA Employees access CDRH Qualtrics through Single Sign-On. During initial account setup select internal FDA Users log in using email address (business) and password (user credentials).</p> <p>The information is stored in accordance with the National Archives and Records Administration (NARA) records schedule.</p>
<b>PTA 05A:</b>	Are user credentials used to access the system?	Yes
<b>PTA 05B:</b>	Please identify the type of user credentials used to access the system.	<p>HHS User Credentials</p> <ul style="list-style-type: none"> <li>HHS/OpDiv PIV Card</li> <li>HHS Email Address</li> </ul> <p>Non-HHS User Credentials</p> <ul style="list-style-type: none"> <li>Password</li> </ul>

<b>PTA 06:</b>	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.	<p>CDRH manages Qualtrics, a survey-as-a-service operation, for the CDRH center internally and externally. CDRH collects information related to customer satisfaction levels stakeholders both inside FDA/CDRH and external, including the medical device industry, academia, patient groups, health professionals, consumers and anyone that interacts with CDRH. These voluntary satisfaction surveys are anonymous and there is no collection of information to categorize survey respondents. The surveys enable CDRH to: (1) determine stakeholder satisfaction ratings; (2) identify and help monitor trends around specific areas of satisfaction or dissatisfaction; and (3) identify areas for process improvement and improve them.</p> <p>The names of FDA Employees and Direct Contractors are collected to track the customer service responses back to the Center for quality assurance purposes.</p> <p>FDA Employees access CDRH Qualtrics through Single Sign-On. During initial account setup, select internal FDA Users log in using email address (business) and password (user credentials).</p>
<b>PTA 07:</b>	Does the system collect, maintain, use, or share PII?	Yes
<b>PTA 08:</b>	Does the system include a website or online application?	Yes
<b>PTA 08A:</b>	Provide the URL(s).	<p><a href="https://cdrh.gov1.qualtrics.com/">https://cdrh.gov1.qualtrics.com/</a></p> <p><a href="https://cdrh.gov1.qualtrics.com/jfe/form/SV_dasAYoa4Vp0zKYK?&amp;ORGID=100017&amp;S=1&amp;E=2">https://cdrh.gov1.qualtrics.com/jfe/form/SV_dasAYoa4Vp0zKYK?&amp;ORGID=100017&amp;S=1&amp;E=2</a></p> <p>Survey URLs always have "/jfe/form/SV_" followed by the survey form ID. The S= and E= are other internal flags used for categorizing responses.</p>
<b>PTA 08B:</b>	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes
<b>PTA 09:</b>	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.	<p>This site enables up to nine users from CDRH Quality Management and Operational Excellence (QMOE) to create and manage surveys for customer feedback and continuous improvement. The site also enables analysis of the collected data.</p> <p>FDA Employees access the website through Single Sign-On. During initial account setup select internal FDA Users log in using email address (business) and password.</p> <p>External users access the web site through public URLs that directs them to the FEDRAMP system to complete the survey.</p>
<b>PTA 10:</b>	Does the website have a posted privacy notice?	Yes
<b>PTA 11:</b>	Does the website contain links to non-federal government websites external to HHS?	No
<b>PTA 12:</b>	Does the website use web measurement and customization technology?	No

<b>PTA 13:</b>	Does the website have any information or pages directed at children under the age of thirteen?	No
<b>PTA 14:</b>	Does the system have a mobile application?	No
<b>PTA 20:</b>	Are any third-party websites or applications (TPWA) associated with the system?	No
<b>PTA 21:</b>	Does this system use artificial intelligence (AI) tools or technologies?	No

### Privacy Impact Assessment

#### Privacy Impact Assessment

<b>PIA 22:</b>	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)
<b>PIA 23:</b>	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
<b>PIA 24:</b>	Indicate the approximate number of individuals whose PII is maintained in the system.	<100
<b>PIA 25:</b>	For what primary purpose is the PII used?	The FDA uses PII to provide FDA Employees with system access. Additionally, the names of FDA Employees and Direct Contractors provided by anonymous survey respondents are used to address customer service feedback and for quality assurance purposes. The names of FDA Employees and Direct Contractors provided through survey responses enable the correlation of the customer feedback with specific organizational units.
<b>PIA 26:</b>	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	Not applicable (N/A)-The FDA makes no secondary use of the PII.
<b>PIA 28:</b>	Identify legal authorities, governing information use and disclosure specific to the system and program.	The legal authorities that govern information use and disclosures specific to the system and program are:  Section 903 of the FD&C Act, codified at 21 U.S.C. § 393, authorizes the FDA to conduct research relating to foods, drugs, cosmetics, medical devices, and tobacco products in carrying out its statutory responsibilities.  21st Century Cures Act (2016): Focused on advancing medical innovation through process reforms.  Food and Drug Administration Amendments Act (FDAAA, 2007): Authorizes surveys and data collection for policy decisions, such as understanding target audiences or behaviors prior to rulemaking.
<b>PIA 29:</b>	Are records in the system retrieved by one or more PII data elements?	No

<b>PIA 30:</b>	Identify the sources of PII in the system.	Government Sources Within the OPDIV Non-Government Sources Private Sector
<b>PIA 31:</b>	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
<b>PIA 31A:</b>	Provide the information collection approval number(s) and expiration date(s).	OMB Control No. 0910-0360 Expires 10/31/2026
<b>PIA 32:</b>	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
<b>PIA 33:</b>	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
<b>PIA 34:</b>	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.	Survey respondents are never asked to provide PII about themselves. However, some surveys may request that anonymous respondents provide the names of FDA Employees or Direct Contractors. Providing these names is optional for survey respondents. FDA Employees and Direct Contractors consent to having their names provided as part of their official duties.
<b>PIA 35:</b>	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 FDA changes its practices regarding the collection or handling of PII related to CDRH Qualtrics, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include email to individuals, adding or updating online notices or forms, or other available means to inform the individual.
<b>PIA 36:</b>	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.	The processes in place to resolve an individual's concerns when their PII has been inappropriately obtained, used, or disclosed include feedback mechanisms within surveys. These surveys contain feedback links that allow users to submit tickets in the system, which triggers investigation and resolution of complaints. Additionally, surveys provide links that enable users to request removal of their own PII.  Individuals may also contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and other agency offices, via email, phone, and standard mail avenues (all listed on fda.gov and the FDA intranet). In the event of a suspected incident or data breach, FDA personnel must immediately report this information without delay to the FDA's CIOCC.

<p><b>PIA 37:</b></p>	<p>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.</p>	<p>The process in place for periodic reviews of PII to ensure data integrity is to verify and validate all data, limit data access and permissions, perform regular access audits, and ensure that the system periodically backs up the data in its storage locations.</p> <p>Data availability is ensured by using role-based access control to provide users with all data necessary to perform their individual work.</p> <p>Data relevancy is ensured by regularly removing user information for those who no longer need access to the system. The system also monitors for PII in data provided by survey respondents and warns users to remove it. If PII is entered, the system is configured to redact the information, except in the case of specific questions requesting the name of internal employees.</p> <p>Accuracy of PII is ensured by collecting the information directly from users and having users verify that their information is correct.</p>
<p><b>PIA 38:</b></p>	<p>Identify who will have access to the PII in the system.</p>	<p>Users Administrators Contractors</p>
<p><b>PIA 38A:</b></p>	<p>Select the type of contractor.</p>	<p>HHS/OpDiv Direct Contractors</p>
<p><b>PIA 38B:</b></p>	<p>Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?</p>	<p>Yes</p>
<p><b>PIA 39:</b></p>	<p>Provide the reason why each of the groups identified in 38 needs access to PII.</p>	<p>Administrators require access to PII about users to manage user accounts, surveys, and datasets and to convert names to organization codes.</p> <p>Users: Data Analysts are users that access PII to perform analyses of collected survey responses and to convert PII (names) to organization codes. The names of FDA Employees and Direct Contractors may be also accessible to data analysts when developing dashboards for the data. PII is not exposed in the dashboards. In some instances, the data analyst may be an administrator.</p> <p>Contractors: FDA Direct Contractors may be users and administrators.</p>
<p><b>PIA 40:</b></p>	<p>Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.</p>	<p>All system users (data analysts and administrators) with access to data in the system will be able see any PII that is in survey responses. The number of system users is limited to a maximum of nine individuals that have completed PII and Privacy training. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access).</p>

<b>PIA 41:</b>	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.	Access is limited to a maximum of nine internal users that require access to complete his/her job. The scope of access is restricted based on role-based permissions.
<b>PIA 42:</b>	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 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 Digital Transformation (ODT) verifies that individuals successfully complete the training.
<b>PIA 43:</b>	Describe the training system users receive above and beyond general security and privacy awareness training.	Training is provided by the software developer and included as part of the software license. CDRH may develop additional training for the system. Additional privacy training and guidance is available via the FDA Privacy Office.
<b>PIA 44:</b>	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).	<p>The applicable records retention schedules are: General Records Schedule (GRS) 5.2 Item 010, Transitory records. Disposition: Temporary. Destroy when no longer needed for business use, or according to agency predetermined time period or business rule.</p> <p>GRS 3.2, Item 031 System Access Records. Systems Requiring Special Accountability for Access. Disposition: Temporary. Destroy six years after password is altered or user account is terminated, but longer retention is authorized if required for business use.</p>

**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.

CDRH officials ensure the system adheres to agency established security controls using personal identity verification (PIV)/Smart card login and/or single sign-on (SSO).

Administrative safeguards include user training; role-based restrictions; supervisor approval prior to user access; 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

<b>Privacy Analyst Review Decision:</b>	Approved	<b>Privacy Analyst Review Date:</b>	11/5/2025
<b>Privacy Analyst Review Comments:</b>		<b># of Days - PA Review:</b>	0

### SOP Review

<b>SOP Review Decision:</b>	Approved	<b>SOP Review Date:</b>	11/5/2025
<b>SOP Review Comments:</b>	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.	<b># of Days - SOP Review:</b>	0

### Agency Privacy Analyst Review

<b>Agency Privacy Analyst Review Decision:</b>	Approved	<b>Agency Privacy Analyst Review Date:</b>	11/26/2025
<b>Agency Privacy Analyst Review Comments:</b>	Reviewer: Nestor Villafuerte 11/26/2025 This PIA is ready for SAOP review and approval.	<b># of Days - APA Review:</b>	21

### SAOP Review

<b>SAOP Review Decision:</b>	Approved	<b>SAOP Review Date:</b>	12/9/2025
<b>SAOP Review Comments:</b>		<b># of Days - SAOP Review:</b>	13

### SAOP Signature

Date	User	Type	Name	Original Value	New Value
12/9/2025 2:13 PM	BAUR, VANESSA	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
No Records Found				