PTA / PIA: FDA - DTAPPS - QTR2 - 2026 - FDA5271403

Created Date: 6/22/2026 6:13 PM Last Updated: 7/2/2026 6:00 PM

General Information

PTA / PIA Name:	FDA - DTAPPS - QTR2 - 2026 - FDA5271403	**PTA / PIA ID:**	4586884
Component Name:	FDA - CDRH DT Applications	**ATO Boundary Name:**	CDRH Regulatory Review
Overall Status:	Complete	**# of Days - Open:**	17
Submitter:		**Submit Date:**	6/22/2026
Next Assessment Date:	07/01/2029	**Expiration Date:**	7/1/2029
Office:		**OpDiv:**	FDA
Security Categorization:	High		
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.	9/22/2025
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	Velayudhan Rajan
PTA 01A:	POC Title and Organization	System Owner FDA/CDRH
PTA 01B:	POC Email Address	Velayudhan.Rajan@fda.hhs.gov
PTA 01C:	POC Phone Number	301-796-0057
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's (FDA) has made no changes to this component since the last Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) 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.	The Center for Devices and Radiological Health (CDRH) Digital Transformation (DT) Applications (DTAPPS) is a comprehensive web-based portal system designed to support the Food and Drug Administration's (FDA) mission of regulating medical devices and protecting public health. Prior to marketing a medical or radiological device, manufacturers must seek FDA approval of their products, and depending on the regulatory class of the device, various types of premarket submissions are submitted to CDRH for scientific review and agency decision-making. DTAPPS serves two distinct user groups with different access methods and functionalities. The external users consist of medical device industry representatives who are responsible for submitting detailed medical device information for approval and tracking their device submissions through multiple stages of review after submission. The internal users include FDA CDRH medical device reviewers and Direct Contractors who review submissions, identify previously submitted devices comparable to those under review, flag potential issues with device approval, and ultimately approve or reject requests for device approval. System access is secured through different authentication mechanisms depending on user type. External industry users access the system through publicly accessible Uniform Resource Locators (URLs) and must authenticate via an Okta portal with multi-factor authentication (MFA) for enhanced security. Internal FDA users, including employees and Direct Contractors, access the system using Single Sign-On (SSO) credentials tied to their HHS username and password, which pulls information from existing FDA systems including the Enterprise Authentication Service for Employees (EASE) for Human Resources (HR) data, SSO username, and Active Directory information. All access utilizes Security Assertion Markup Language (SAML) 2.0 protocol, which is an agency-approved standard to secure applications. DTAPPS provides holistic medical data review management through several integrated components that work together to modernize and streamline the device review process. The system's primary functions are carried out through the Customer Collaboration Portal (CCP) and the Decision Management Portal (DMP), supported by a Modern Analytics platform and Enterprise Integration capabilities. The CCP serves as a web interface to facilitate collaboration with external medical device industry representatives, enabling them to submit detailed medical device

		information for approval, track their device submissions through multiple stages of review, and maintain continuous two-way communication with FDA reviewers. This portal modernizes interaction between CDRH and industry through an online digital experience that facilitates the exchange of ideas and information, creates transparency via a submission dashboard that improves electronic submission capability, and updates current intake processes to be more comprehensive, efficient, and user-friendly. The DMP functions as a digital workbench that becomes the central access point for internal FDA CDRH medical device reviewers to perform and manage their day-to-day responsibilities and activities. Through this portal, reviewers can identify previously submitted devices comparable to those under review, flag potential issues with device approval, access real-time collaboration tools, utilize comprehensive search capabilities, and ultimately approve or reject requests for device approval. The DMP provides a consistent user experience that integrates across applications, removes duplicate data entry, provides alerts and notifications, and displays uniform data while also managing user workload, status, operations management, and tracking submissions through the entire FDA review and approval pipeline. Together, these capabilities provide the Center's reviewer community with a scalable, cost-effective, and transformative solution that enables the rapid processing, validation, management, and analysis of data across the medical device lifecycle. The system supports the Department of Health and Human Services (HHS) mission by simplifying the management and review of required documents for the regulation of the safety and effectiveness of a wide range of medical devices, ultimately enabling better collaboration between FDA and industry while streamlining the decision-making process that protects public health.
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.	The CDRH DT Applications system collects, maintains, and shares various types of information to support the medical device review and approval process. The system collects contact information including the full name of the submitter, full names of alternate contacts for submission, organization name when applicable, work email address, work phone number, and mailing address. For voluntary submitters, this could potentially include home address and phone number. User credentials and authentication information are also collected, including HHS username and password for internal users, username and password for external users. Single Sign-On (SSO) username, Active Directory information, and information from the Enterprise Authentication Service for Employees (EASE), including Human Resources (HR) data for internal users.

The system maintains regulatory and submission data essential to the device review process. This includes medical device information submitted for FDA approval, device labeling organization's regulatory point of contact information, and designated support point of contact information, which may represent a role or office rather than an individual. Medical Device Reporting (MDR) data is collected, including both non-redacted and redacted narrative text, along with submitter company or organization information and premarket submission documentation and tracking information. The system also includes free text fields where personally identifiable information (PII) could potentially be provided, though such information is not specifically requested or required. Additional operational data includes submission status and tracking information, workload management data, and operations management information.

The system handles several categories of potentially sensitive information with varying levels of security impact. Trade secrets are categorized as having High confidentiality impact, while Confidential Commercial Information, PII, Protected Health Information (PHI), Pre-decisional Information, and Adverse Event Data are all categorized as having Moderate confidentiality impact. The integrity impact for most information types is Moderate, with trade secrets having Moderate integrity impact specifically because the data collected is not considered the source of truth. Availability impact is generally categorized as Moderate for sensitive information types and Low for most other information categories.

Retention and destruction of information is managed according to the authorized FDA and CDRH Records Retention Schedule and Information Technology (IT) procedures. CDRH follows the appropriate Records Retention schedule depending on the submission type and applicable records control schedule. File Code 2300, which covers Investigational and Pre-Investigational Device Exemptions (Investigational Device Exemptions and Pre-Investigational Device exemptions), follows National Archives and Records Administration (NARA) Citation N1-088-08-1, Item 2.3, and consists of temporary records that are destroyed when no longer needed or after 20 years, whichever is later. File Code 2400, covering Premarket Approval Applications (PMAs), follows NARA Citation N1-088-08-1, Item 2.4, and consists of temporary records destroyed when no longer needed or after 30 years, whichever is later. File Code 2500, which addresses Premarket Notification (510(k)) submissions, follows NARA Citation N1-088-08-1, Item 2.5, and consists of temporary records destroyed when no longer needed or after 20 years, whichever is later. Other applicable schedules include General Records Schedule 20, item 2a4, and FDA file codes in the 2000-2700 family. These schedules typically call for deletion of records when no longer needed for

		business and regulatory purposes, or after 20, 25, or in some cases 30 years, whichever is later. CDRH is currently conducting records retention enforcement planning to ensure compliance with these retention requirements.
PTA 05A:	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.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	The CDRH DT Applications system utilizes CDRH Okta Software as a Service (SaaS) as the enterprise identity management platform for managing access and authentication for external users. CDRH Okta is a FedRAMP authorized cloud service that serves as the repository for external user accounts, user credentials, and user role assignments, which determine access across all applications in the platform. This is a CDRH-specific implementation of Okta SaaS deployed to support DTAPPS. External user credentials, including usernames and passwords, are stored and managed within Okta and are not independently collected or stored within the DTAPPS application itself. For internal FDA users, authentication is managed through existing FDA infrastructure. The DMP displays user profile information drawn from existing FDA systems, including EASE for HR data, SSO username, and Active Directory information. The DMP only displays this information; it does not gather, store, or otherwise process it independently. Internal user credentials remain in those source systems. Okta is administered by two classes of users: administrators and developers. Administrators assign and revoke the developer role, while developers manage configuration and can create, delete, and manage the DTAPPS user accounts that are maintained within Okta. User access is restricted by MFA using SMS and email, and other authentication factors can be enabled from the Security tab of the Okta admin dashboard. The production environment is accessible at https://fda-cdrh.okta.com, while the pre-production environment is accessible at https://fda-cdrh-pre-prod.oktapreview.com.
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.	The CDRH DT Applications system collects, maintains, and shares various types of information to fulfill FDA's regulatory mandate under the 1976 Medical Device Amendments to the Food, Drug, and Cosmetic Act, which requires the FDA to collect and analyze manufacturer data for medical device approval and safety monitoring. **Information Collected About External Industry Users (Device Manufacturers and Submitters)** *Contact Information (Name, Phone Number, Email Address, Organization):* This information is collected to assist FDA personnel with requesting and obtaining additional information about

product submissions as needed. The system collects the full name of the submitter, work email address, and work phone number to enable FDA reviewers to communicate with the appropriate point of contact when questions arise during the review process. The submitter's organization information is collected to assist FDA personnel with finding alternate contacts for requesting or obtaining additional information if the specific submitter cannot be reached. For device labeling organizations, the system collects the regulatory point of contact information, which is the person to whom FDA should address correspondence, as well as the designated support point of contact, which is the person or organization that members of the public may contact with questions or other concerns. The support point of contact information may represent a role or office rather than an individual and therefore may not always constitute PII.

Voluntary Submitter Information: Voluntary submitters could potentially provide home address, home phone number, and personal email address. This information is collected to maintain contact with submitters who may not have a business address or who choose to submit information independently.

External User Credentials: Usernames and passwords for external users are collected to authenticate users and control access to the DTAPPS system. These credentials are stored and managed within the CDRH Okta SaaS platform, which serves as the enterprise identity management system for DTAPPS. Collection of these credentials is necessary to verify the identity of external users and to enforce role-based access controls that determine what information and functions each user may access within the CCP.

Medical Device Submission Data: This information is collected to enable FDA to fulfill its regulatory responsibility to review and approve medical devices before they can be marketed. Depending on the regulatory class of the device, various types of premarket submissions are submitted to CDRH for scientific review and agency decision-making. Submissions may contain trade secrets, Confidential Commercial Information, and Adverse Event Data, all of which are collected as part of the mandatory regulatory submission content required under the Medical Device Amendments to the Food, Drug, and Cosmetic Act and related regulations. These data categories are handled in accordance with their respective confidentiality impact levels as described in PTA 05.

MDR Data: MDR data, including non-redacted and redacted narrative text, is collected to support FDA's post-market safety surveillance responsibilities. This narrative text may contain PII such as patient or reporter information. This data is collected under FDA's legal authority to monitor

the safety of marketed medical devices.

Free Text Field Information: The submission form includes several open-answer text boxes in which PII could potentially be provided. While no PII beyond the contact information specified above is specifically requested or required, it may enter the DMP through these free text fields as submitters provide detailed information about their device submissions.

Information Collected About Internal FDA Users (Employees and Direct Contractors)

User Authentication Information (SSO Username, Active Directory Information, EASE Data): This information is used to authenticate internal users and provide them with appropriate role-based access to the system. The DMP displays user profile information drawn from existing FDA systems, including EASE for HR data, SSO username, and Active Directory information. This information is necessary to verify that users are authorized FDA personnel or contractors and to assign them appropriate permissions based on their roles and responsibilities. DTAPPS does not independently store this information; it remains in the source systems.

Workload and Operations Management Data: Information about reviewer workload, submission status, and operations management is collected to enable efficient management of the device review process and to track submissions through the entire FDA review and approval pipeline.

Information Sharing with Other Systems

The system shares information with other FDA systems to support the integrated medical device review process. CDRH DTAPPS connects to the CTS, which is managed by CSTAR, via a MuleSoft API. The DMP homepage displays information from CTS but does not gather or otherwise process it independently. The system also shares information with Documentum for document management purposes. Files that are successfully scanned through the electronic submission process are moved to Documentum via a secure and authenticated API managed by CDRH MuleSoft.

Additionally, the system has interconnections with CDRH Center Ad-Hoc Reporting System (CARS), CDRH Center Tracking System (CTS), and CDRH Center Electronic Submissions (CeSub) to facilitate the comprehensive tracking and management of medical device submissions throughout their lifecycle. These interconnections enable the system to provide holistic medical data review management and ensure that all relevant information is available to reviewers when making regulatory decisions about device safety and effectiveness. CDRH CARS, CTS, and CeSub are the

		subject of a separate assessment. The collection and sharing of this information is essential to CDRH's mission of protecting public health by ensuring that medical devices are safe and effective before they reach the market, and by monitoring device safety through adverse event reporting and other post-market surveillance activities.
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).	The following URLs are accessible by the public: Production Environment: Customer Collaboration Portal (CCP): https://ccp.fda.gov/prweb/PRAuth/app/default/extsso Electronic Submission Component: https://ccp-aws.fda.gov/ Pre-Production Environment: Customer Collaboration Portal (CCP) Pre-Production: https://ccp-mig.preprod.fda.gov/prweb/PRAuth/app/default/extsso Electronic Submission Component Pre-Production: https://ccp-aws.preprod.fda.gov/ These publicly accessible URLs allow external medical device industry representatives and manufacturers to reach the login pages where they must authenticate through an Okta portal with multi-factor authentication (MFA) to access the system. The pre-production URLs are used by FDA employees and contractor testers for User Acceptance Testing (UAT) and troubleshooting purposes, but they remain externally accessible to support ongoing testing activities.
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 CDRH DT Applications website serves dual purposes for both agency and industry users in support of the medical device review and approval process. The Customer Collaboration Portal (CCP) is used by industry users to interface with FDA reviewers about their device submissions, enabling them to submit detailed medical device information for approval, track their submissions through multiple stages of review, and maintain continuous two-way communication with FDA personnel. The Decision Management Portal (DMP) is used by FDA personnel to submit product information for review and approval, manage their workload, access real-time collaboration tools, and make regulatory decisions about device applications. Together, these portals modernize the interaction between CDRH and industry through an online digital experience that facilitates

the exchange of ideas and information, creates transparency through submission dashboards, and updates current intake processes to be more comprehensive, efficient, and user-friendly.

The website is accessible to two distinct user groups. External users consist of medical device industry representatives and manufacturers who need to submit device information to FDA and track the status of their submissions. Internal users include FDA employees and Direct Contractors who serve as CDRH medical device reviewers and are responsible for evaluating submissions, identifying comparable previously submitted devices, flagging potential issues, and ultimately approving or rejecting device approval requests.

Access to the website requires authentication and varies based on whether users are accessing production or pre-production environments. All access requires login via an Okta portal, with different authentication requirements for external versus internal users. External industry users must use multi-factor authentication (MFA), while internal agency users authenticate through Single Sign-On (SSO). Security Assertion Markup Language (SAML) 2.0 protocol is used to secure all applications, which is an agency-approved standard.

Production Environment URLs:

For the Customer Collaboration Portal, external users access the production environment at https://ccp.fda.gov/prweb/PRAuth/app/default/extsso. For the Decision Management Portal, internal users access the production environment at https://dmp.fda.gov/prweb/PRAuth/sso. The electronic submission component is accessible at https://ccp-aws.fda.gov/.

Pre-Production Environment URLs:

The CDRH DT Applications pre-production URLs are used by FDA employees and contractor testers to troubleshoot issues that only present with external access and not internal access. For the Customer Collaboration Portal pre-production environment, users access https://ccp-mig.preprod.fda.gov/prweb/PRAuth/app/default/extsso. For the Decision Management Portal pre-production environment, users access https://dmp.preprod.fda.gov/prweb/PRAuth/sso. The electronic submission pre-production environment is accessible at https://ccp-aws.preprod.fda.gov/. Continuous external access to the CCP pre-production environment is maintained to allow User Acceptance Testing (UAT) testers to perform external UAT testing in support of ongoing DTAPPS sprint release activities, as not allowing continuous access would cause significant delays in the DTAPPS production release schedule.

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 (Personal) Mailing Address (Personal) Phone Numbers (Personal) Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Other Other

PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	The following additional types of PII may be collected, maintained, or shared by the system: External User Credentials: Username and password credentials are collected for external users and are stored and managed within the CDRH Okta SaaS platform, which serves as the enterprise identity management system specifically implemented to support DTAPPS. These credentials are not independently stored within the DTAPPS application itself. Internal User Profile Data (Displayed Only): For internal FDA users, the DMP displays SSO username, Active Directory information, and HR data drawn from EASE. This information is maintained in those source systems and is not independently collected or stored by DTAPPS. MDR Narrative Text: Non-redacted MDR narrative text collected for post-market safety surveillance purposes may contain PII, such as patient or reporter identifying information, even though such information is not specifically solicited. Free Text Field PII: The submission forms include several open-answer text boxes in which PII could potentially be provided by submitters. While no PII beyond the contact information specified above is specifically requested or required, it may enter the system through these free text fields as submitters provide detailed information about their device submissions. It is important to note that while the system has the capability to collect certain types of PII through free text fields and MDR narrative text, not all of this information is specifically requested or required. The primary PII collected relates to contact information necessary for FDA personnel to communicate with submitters regarding their medical device submissions and to fulfill the agency's regulatory responsibilities.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
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 primary purpose for which PII is used in the CDRH DT Applications system is to enable FDA employees and Direct Contractors to process and correspond with submitters (industry points of contact) regarding their medical device submissions to the FDA. Specifically, PII is collected to assist FDA personnel with requesting and obtaining additional information about product submissions as needed during the review process. Contact information, including names, phone numbers, and email addresses, allows FDA reviewers to communicate directly with the appropriate individuals when questions arise, clarifications are needed, or additional documentation is required. The submitter's organization information is also used to help FDA personnel find alternate contacts if the specific submitter cannot be reached, ensuring continuity in the review process. MDR narrative text, which may incidentally contain PII, is collected to support FDA's post-market safety surveillance responsibilities under applicable medical device reporting regulations. This use of PII supports FDA's regulatory mandate under the 1976 Medical Device Amendments to the Food, Drug, and Cosmetic Act to collect and analyze manufacturer data, conduct scientific reviews of medical device submissions, and make informed regulatory decisions about device safety and effectiveness before products can be marketed to the public.
PIA 26:	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 collected, maintained, or shared in the CDRH DT Applications system. All PII in the system is used solely for the primary purpose of enabling FDA employees and Direct Contractors to process and correspond with submitters regarding their medical device submissions to the FDA. The information is not used for testing, training, research, or any other secondary purposes beyond the direct support of the medical device review and regulatory decision-making process.

PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The following legal authorities govern information use and disclosures specific to the CDRH DT Applications system and program: Medical Device Regulatory Authorities: The Medical Device Amendments to the Food Drug and Cosmetic Act, including the Medical Device Amendments 21 U.S.C. sections 360, 360c, 360e, 360i, 360j, 360l, 510(k), 515(c), 515(d), 515(f), 519, 520(g), 520(m), and 564 The Federal Food, Drug, and Cosmetic Act, section 519(f) Mammography and Medical Device Safety Authorities: Mammography Quality Standards Act Regulations (MQSA), 42 U.S.C. 263b Safe Medical Device Act of 1990 (SMDA), 21 U.S.C. 301, 42 U.S.C. 263b-n Medical Device Reporting Regulations: Medical Device Reporting regulations at 21 CFR 803, 803.32, and 803.40; 21 U.S.C. 352, 360, 360i, 360j, 371, 174 Radiological Health Regulations: The Radiological Health regulations CFR 1002.1(c)(4), 1002.10-1002.13, 1002.20, 1020.30(d), and 1020.30(d)(1), as well as Table 1 in 21 CFR 1002.1(b); 21 U.S.C. 352, 360, 360i, 360j, 360hh-ss, 371, 174 These legal authorities establish FDA's mandate to collect and analyze manufacturer data, conduct scientific reviews of medical device submissions, monitor device safety through adverse event reporting, and regulate radiological health products. They provide the legal foundation for the collection, use, maintenance, and disclosure of information within the CDRH DT Applications system in support of the agency's mission to protect public health by ensuring the safety and effectiveness of medical devices.
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 Hard Copy Mail/Fax Online Government Sources Within the OPDIV Non-Government Sources Members of the Public Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No

PIA 31B:	Explain why an OMB information collection approval number is not required.	The information collection activities conducted through the CDRH DT Applications system are conducted under FDA's existing statutory authorities for medical device review and approval, as established by the Medical Device Amendments to the Food, Drug, and Cosmetic Act and related regulations. To the extent that any information collections conducted through DTAPPS are subject to the Paperwork Reduction Act, those collections are covered by existing OMB-approved information collection instruments associated with the underlying regulatory submission types (such as 510(k), PMA, and MDR submissions), which are maintained separately by the relevant program offices. DTAPPS serves as the modernized digital platform through which these statutorily mandated collections are received and processed, rather than as an independent discretionary information collection that would require separate OMB clearance.
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.	Individuals serving as points of contact responsible for submitting information on behalf of manufacturers are notified that their information will be collected through the system's privacy notice posted on the website. The CDRH DT Applications website has a posted privacy notice that informs users about the collection and use of their PII. Participation in the submission process is voluntary. However, once an individual or organization elects to submit a medical device application, the provision of contact PII is required to complete the submission process, as this information is necessary for FDA personnel to communicate with submitters and fulfill the agency's regulatory mandate. There is no option to opt out of PII collection while still completing the submission process. Individuals serving as points of contact may update or correct their contact information by advising the FDA via phone, email, or during the submission of records to FDA. The collection of this information is authorized under the Medical Device Amendments to the Food, Drug, and Cosmetic Act and related regulations, which require FDA to collect and analyze manufacturer data for medical device approval and safety monitoring.

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 the FDA's privacy practices change or FDA changes its collection, use, or sharing of PII data in the CDRH DT Applications system, the individuals whose PII is in the system will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a formal process involving written and/or electronic notice, or informal processes such as email notice to the individuals. Additionally, as regulations change mandating the collection of PII information, there is an open period where the public can submit comments on the regulation. This public comment process provides an opportunity for individuals and organizations to be informed about proposed changes to information collection requirements and to provide feedback before such changes are implemented. The approach to notification is designed to be flexible and tailored to the nature and scope of the changes being made. The FDA will select the notification method that is most efficient and effective based on the specific circumstances, ensuring that affected individuals are appropriately informed about material changes to how their PII is collected, used, or shared. This could range from formal written notifications for significant policy changes to more informal email communications for minor updates, depending on what is most appropriate for keeping individuals informed about changes that affect their privacy.

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.	Individuals may contact FDA/CDRH by phone, mail, or email using the contact information provided on the fda.gov site and the specific fda.gov web pages associated with the various CDRH DT Applications submissions if they have concerns about how their PII has been obtained, used, or disclosed, or if they believe their PII is inaccurate. Additionally, individuals may contact the FDA Privacy Office by using the contact information provided on FDA.gov as well as the FDA intranet. In the event of a report of possible compromise of PII in the system, the FDA security team, Privacy Office, and relevant program and system officials will initiate the FDA's incident/breach response process. This coordinated response ensures that any potential privacy or security incidents are properly investigated and addressed according to established FDA protocols. For concerns about the accuracy of PII, individuals serving as points of contact responsible for submitting information on behalf of manufacturers may update or correct their contact information by advising the FDA via phone, email, or during the submission of records to FDA. Since PII is provided voluntarily by the submitter in order to complete the submission process, the submitter is responsible for providing accurate information. Accuracy is ensured by the submitter at the time of reporting, and submitters may correct or update their information themselves by sending an updated submission via US Postal Mail, Fax, and/or Compact Disc (CD)/Digital Versatile Disc (DVD). This multi-faceted approach provides individuals with multiple channels to raise concerns and ensures that both routine corrections and potential security incidents are handled through appropriate processes with the involvement of relevant FDA offices and officials.
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.	PII is provided voluntarily by the submitter in order to complete the submission process. The submitter is responsible for providing accurate information, and accuracy is ensured by the submitter at the time of reporting. Submitters may correct or update their information themselves by sending an updated submission via US Postal Mail, Fax, and/or CD/DVD. This approach places the responsibility for data accuracy on the individuals who are most knowledgeable about their own contact information and organizational details. Integrity and availability of PII are protected by security controls selected and implemented as part of the Authorization to Operate (ATO) process. National guidance concerning the ATO process is followed, appropriate to the system's level of risk as determined using the National Institute of Standards and Technology's (NIST) Federal Information Processing Standards (FIPS) 199. The system has been categorized as a high impact information system, which requires robust security

		controls to protect the confidentiality, integrity, and availability of the information it contains. CDRH performs semi-annual reviews to evaluate user access to the system. These reviews help ensure that only authorized individuals maintain access to PII and that access privileges remain appropriate based on users' current roles and responsibilities. This periodic review process supports both data integrity and security by identifying and addressing any inappropriate or outdated access permissions. One of the controls implemented includes information system backups reflecting the requirements in contingency plans as well as other agency requirements. These backups support data availability and integrity by ensuring that PII can be recovered in the event of system failures, disasters, or other incidents that could compromise data availability. The relevancy of PII is maintained through the system's operational purpose and the records retention schedule. Information remains relevant as long as it is needed to support active medical device submissions and FDA's regulatory decision-making processes. Once information is no longer needed for business and regulatory purposes, it is disposed of according to the authorized FDA and CDRH Records Retention Schedule, which typically calls for deletion of records when no longer needed or after the applicable retention period (20, 25, or 30 years depending on the submission type), whichever is later. This comprehensive approach ensures that PII in the system maintains its integrity, remains available when needed, stays accurate through submitter responsibility and correction mechanisms, and remains relevant to FDA's regulatory mission throughout its lifecycle in the system.
PIA 38:	Identify who will have access to the PII in the system.	Users 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: PII is provided voluntarily by the submitter in order to complete the DMP submission process. External users (medical device industry representatives and manufacturers) need access to their own PII to submit device applications, update their contact information, and track their submissions through the FDA review process. They are technically restricted to accessing only their own PII and submission information. Internal users (FDA CDRH medical device reviewers and staff) need access to submitter PII to process medical device submissions, request or obtain additional information about product submissions as needed, communicate with submitters when questions arise during the review process, and make informed regulatory decisions about device safety and effectiveness. Developers and Contractors: Developers and contractors in this system are HHS/OpDiv Direct Contractors who assist in the development, maintenance, and operation of the system. Access to PII is required for troubleshooting and maintenance of the overall system, including diagnosing technical issues, testing system functionality, performing system updates and enhancements, and ensuring that data flows properly through the various integrated components of the CDRH DT Applications platform. Both regular and privileged users may be Direct Contractors. All contractor access to PII is governed by role-based access control (RBAC), need-to-know principles, and least privilege policies, and is subject to the same Federal Acquisition Regulation (FAR) privacy clauses and contractual privacy provisions that apply to all HHS Direct Contractors. All access to PII by these groups is governed by RBAC, need-to-know principles, and least privilege policies to ensure that individuals only access the minimum amount of PII necessary to perform their specific job functions.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to the CDRH DT Applications system is based on RBAC, need-to-know, and least privilege principles. The system maintenance team utilizes a "need to know" policy for granting access to the PII. Typically, only developers, lead analysts, and privileged users are allowed access to PII either through the web application interface or through the database. The determination of who receives access varies depending on the user category: For Developers and Lead Analysts: The system supervisor determines who receives access to PII. This ensures that access is granted only to those technical personnel who require it to perform system development, troubleshooting, and maintenance functions. For Privileged Users: CDRH business supervisors determine which individuals are permitted access to PII. This ensures that access aligns with business needs and regulatory responsibilities, and that only those with legitimate business purposes can access sensitive information. Each internal FDA Form 3530 (User Access Request Form) submitted by each user to justify access requests is reviewed and vetted thoroughly. This formal request and review process ensures that access is granted only after careful consideration of the individual's role, responsibilities, and legitimate need for access to PII. The use of the FDA Form 3530 provides documentation of access requests and approvals, supporting accountability and audit requirements. This multi-layered administrative approach ensures that access to PII is carefully controlled, properly authorized by appropriate supervisory personnel, and limited to only those individuals who have a demonstrated need to access such information in order to perform their assigned duties.

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.	All authorized system users require access to PII to perform their job functions. However, technical controls are in place to ensure users can only access the minimum amount of information necessary based on their specific roles and responsibilities. For the web application interfaces, there are various user roles for the applications where minimum access rules can be applied. These role-based controls allow the system to restrict what information different categories of users can view and interact with based on their assigned roles. This ensures that users only see the PII that is relevant to their specific job functions within the CCP or DMP. External users (medical device industry representatives and manufacturers) are technically restricted to accessing only their own PII and submission information. They cannot view or access PII belonging to other submitters or organizations, ensuring that industry users only see information related to their own device applications. For developers and lead analysts who require broader access for system maintenance and troubleshooting purposes, access to PII is necessary to perform their job functions. While these users may have more extensive technical access to support system operations, their access is still governed by the administrative procedures and need-to-know policies that limit access to what is required for their specific responsibilities. Each internal FDA Form 3530 submitted by each user to justify access requests is reviewed and vetted thoroughly. This process ensures that the technical access granted aligns with the minimum necessary standard by requiring users to document and justify why they need specific levels of access to perform their duties. These technical methods work in conjunction with the administrative procedures and RBAC framework to implement the principle of least privilege, ensuring that while authorized users can access the PII they need, they are prevented from accessing information beyond what is necessary for their job functions.

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.	The FDA makes it mandatory for all FDA personnel and Direct Contractors to take Information Technology (IT) security and privacy training annually. A portion of this training is dedicated to the protection and handling of PII overall for the agency. Completion of annual Computer Security Awareness Training (CSAT) is tracked by the Office of Digital Transformation (ODT). This tracking ensures that all system users, including system owners, managers, operators, contractors, and program managers, remain current with their training requirements and are aware of their responsibilities for protecting the information being collected and maintained in the CDRH DT Applications system. This mandatory annual training program ensures that all personnel who have access to the system understand their obligations to protect sensitive information, including PII, and are aware of current security and privacy policies, procedures, and best practices for safeguarding the data entrusted to them.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	No additional system-specific training is received by users of the CDRH DT Applications system beyond the general security and privacy awareness training. While additional training is available from the FDA Privacy Office for those who may need more specialized guidance, there is no mandatory system-specific training program that goes beyond the general annual security and privacy awareness training requirements.
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).	Retention and destruction of PII is managed according to the authorized FDA and CDRH Records Retention Schedule and IT procedures. CDRH follows the appropriate Records Retention schedule depending on the submission type and applicable records control schedule. CDRH is currently conducting records retention enforcement planning to ensure compliance with these retention requirements. Specific National Archives and Records Administration (NARA) Records Retention Schedules: File Code 2300 — Investigational and Pre-Investigational Device Exemptions (IDEs and PIDs): NARA Citation: N1-088-08-1, Item 2.3 Classification: Temporary records Retention Period: Records are destroyed when no longer needed for business and regulatory purposes, or after 20 years, whichever is later. File Code 2400 — Premarket Approval Applications (PMAs): NARA Citation: N1-088-08-1, Item 2.4 Classification: Temporary records Retention Period: Records are destroyed when no

		longer needed for business and regulatory purposes, or after 30 years, whichever is later. File Code 2500 — Premarket Notification (510(k)): NARA Citation: N1-088-08-1, Item 2.5 Classification: Temporary records Retention Period: Records are destroyed when no longer needed for business and regulatory purposes, or after 20 years, whichever is later. Other Applicable Schedules: Additional schedules that apply to various records in the system include NARA Citation N1-088-08-1, Items 2.1–2.5 and FDA file codes in the 2000–2700 family. System access records are managed under General Records Schedule (GRS) 3.2, Information Systems Security Records, Item 030, which covers systems not requiring special accountability for access (Disposition Authority: DAA-GRS-2013-0006-0003); these are temporary records destroyed when business use ceases. Transitory and intermediary records are managed under GRS 5.2, Transitory and Intermediary Records, Item 20 (Disposition Authority: DAA-GRS-2022-0009-0002); these are temporary records destroyed upon creation or update of the final record, or when no longer needed for business use, whichever is later. General Retention Guidelines: These schedules typically call for deletion of records when no longer needed for business and regulatory purposes, or after 20, 25, or in some cases 30 years, whichever is later. The "whichever is later" provision ensures that records are retained as long as they continue to serve a business or regulatory purpose, even if that extends beyond the specified retention period. This approach balances the need to maintain records for regulatory and legal purposes with the privacy principle of retaining PII only as long as necessary.
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 mandatory annual IT security and privacy training for all FDA personnel and Direct Contractors, which covers the protection and handling of PII. System documentation advises users on proper use of the system and handling of sensitive information. The implementation of Need to Know and Minimum Necessary principles is enforced when awarding access, ensuring that users only receive access to the PII required for their specific job functions. Access to the system is based on RBAC, need-to-know, and least privilege principles. The system maintenance team utilizes a "need to know" policy for granting access to PII, with system supervisors determining access for developers and lead analysts, and CDRH business supervisors determining access for privileged users. Each internal FDA Form 3530 submitted by users to justify access requests is reviewed and vetted thoroughly. Additionally, CDRH performs semi-annual reviews to evaluate user access to ensure

access privileges remain appropriate.

Technical safeguards include MFA for external users accessing the system through the Okta portal, and SSO authentication for internal FDA users. The use of Secure Sockets Layer (SSL) protects data in transit. All data transmitted is protected via Federal Information Processing Standard (FIPS) 140-2 encryption. SAML 2.0 protocol is used to secure all applications, which is an agency-approved standard. Access to application programming interface (APIs) always uses Hypertext Transfer Protocol Secure (HTTPS) and is exclusively routed through the F5 Load Balancer. Authentication and authorization for accessing APIs is managed by API Manager, which enables security policies at the application level and allows platform users to apply specific policies based on use case requirements. MuleSoft Client ID Enforcement Policy restricts API requests to registered client applications only, and JavaScript Object Notation (JSON) Threat Protection policy is in place to protect against malicious JSON in API requests. Files submitted via the CDRH eSubmission Amazon Web Services (AWS) API Gateway are triaged and virus scanned by ClamAV antivirus engine before being moved to Documentum. Security groups are in place to limit CDRH eSubmission AWS API Gateway accessibility to only traffic initiating from authorized CDRH Pega Server IP ranges, and each CDRH Pega API call requires an access key before the API request is accepted. For the web application interfaces, various user roles allow minimum access rules to be applied. Information system backups are performed reflecting the requirements in contingency plans as well as other agency requirements.

All system servers are located at FDA facilities protected by guards and locked facility access. Doors require badge access for entry. Climate controls are maintained to protect server equipment. Other appropriate physical security controls have been selected from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, as determined using FIPS 199. The system has been categorized as a high impact information system, which requires robust physical security controls commensurate with that risk level.

These administrative, technical, and physical controls work together as part of a comprehensive security framework. The controls have been selected and implemented as part of the ATO process, following national guidance concerning the ATO process appropriate to the system's level of risk as determined using NIST FIPS 199. The security controls are documented in the System Security Plan and are subject to regular security assessments to ensure they remain effective in protecting PII and other sensitive information

	maintained in the system.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	6/22/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/22/2026
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:**	6/24/2026
Agency Privacy Analyst Review Comments:	Reviewer: Godisgreat Peters 6/24/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	2

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	7/2/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	8

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/2/2026 2:35 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
PTA 01	BLAND, CRYSTAL	6/23/2026	6/23/2026 Per FDA: The PIA is 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 automatically entering the answer “No,” which is incorrect. **The ATO date is 9/22/2025.** At this time, we are unable to update Archer to reflect the correct answer “Yes.”	6-23-2026 EMAIL_FW_ PTA _ PIA 5271403 is ready for APA Review.pdf CDRH DT Applications SOP approved.pdf