PTA / PIA: FDA - CIMS - QTR2 - 2025 - FDA4915688

Created Date: 4/7/2025 12:24 PM Last Updated: 4/14/2025 4:37 PM

General Information

PTA / PIA Name:	FDA - CIMS - QTR2 - 2025 - FDA4915688	**PTA / PIA ID:**	2980353
Component Name:	FDA - CDRH Information Management Support	**ATO Boundary Name:**	CDRH Regulatory Review
Overall Status:	Complete	**# of Days - Open:**	10
Submitter:		**Submit Date:**	4/4/2025
Next Assessment Date:	04/13/2028	**Expiration Date:**	4/13/2028
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?	No
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.	10/12/2022
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	Rajan Velayudhan
PTA 01A:	POC Title and Organization	CIMS Business Owner
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.	Since the last assessment of this system, FDA has made system enhancements to support the changes of technology, but the agency has made no changes to the way data is collected, handled or stored.
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 purpose of the Center for Devices and Radiological Health (CDRH) Information Management System (CIMS) is to support the management and review of the required documents for the regulation of the safety and effectiveness of a wide range of medical devices. CIMS allows CDRH to monitor the workload; manage the submissions repository; and otherwise support the accomplishment of regulatory and business functions. The CIMS system is a collective of the information technology (IT) systems, supporting components, and initiatives that feature unique medical device-related projects, and/or foster knowledge-based and information-sharing environments. This is accomplished through tools and technologies that support document management, search/discovery, collaboration, and social systems. CIMS is comprised of the following applications: Image 2000+ (with supporting component - I2K SOLR, I2K Download, eBackend, eReference, eService, Postmarket 522 Upload, DCC Electronic Exchange Email Processing Systems (DEEEPS). Documentum Service, and Documentum) and the original standalone application Document Manager (DocMan). Image 2000+ (or I2K+), is the central repository and the official records management system for CDRH. The repository includes document management activities for premarket, compliance, post market, and administrative business processes. The CDRH Image 2000+ system provides a web-based user interface providing authorized users the ability to search and retrieve important submission-related content and documentation from within the CDRH Electronic Document Repository (EDR), in addition to web-based submissions. The operation of the CIMS I2K+ capability requires supporting components (that include modules and standalone applications) that serve a critical role within the CIMS process. These individual components include: The eBackend system that enables electronic access to industry-submitted medical device documentation that is stored in the Documentum repository; The I2K Download system which is a standalone application that enables the user to check out documents from the repository (similar to checking out a book at the library); The eReference component is a module that is executed within the system to provide users the ability to link various types of references to a pre-specified source; The eService application allows users to upload PDF files to the I2K Documentum Repository. The other major capability of CIMS is the DocMan application that serves as the enterprise content management system.

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.	In support of the CDRH device submission process, CIMS is dedicated to the management of the submissions (e.g., required regulatory documentation) and corresponding processes. The information contained in CIMS represents the official record of submissions from manufacturers. This includes Premarket Notifications 510(k), Lead and consults review documents for Pre/Post-Market Approval (PMAs), Investigational Device Exemptions (IDEs), Pre-Submissions, Humanitarian Device Exemption (HDE) requests, product labeling data, medical device reporting, and establishment registration and medical device listing forms. All FDA decision letters, and any supplemental information requested from the manufacturer are stored in the CIMS. In addition to the regulatory documentation listed above, CIMS collects and maintains the following PII information: first and last name, work (business) email address, and work (business) phone number. Additionally, if the sender elects to include it, the e-mail submissions may also contain additional contact information as part of their signature block in the body of the e-mail. This voluntarily submitted information may include job title, work mailing address, and/or work phone and fax numbers. Controlled access to CIMS is granted via Personal Identity Verification PIV card and a single sign-on (SSO) process using multifactor authentication, therefore, user credentials are not collected or stored by the system. CDRH follows the appropriate Records Retention schedule depending on the submission type and applicable records control schedule. Schedules that apply to the various records in the system include NARA citation N1-088-08-1, Items 2.1-2.5; General Records Schedule 20, item 2a4; and FDA file codes in the 2000-2700 family. These 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.
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.	Active Directory.

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.	Under the 1976 medical device amendments to the Food, Drug, and Cosmetic Act, the Food and Drug Administration (FDA) is mandated to collect and analyze manufacturer data related to the safety and efficacy of medical devices before they may be marketed in the United States. CIMS is dedicated to the management of the submissions by manufacturers of this regulatory data (e.g., required regulatory documentation). The information contained in CIMS represents the official record of submissions from manufacturers. CIMS does not itself request or collect PII directly from the subject individuals. Rather, CIMS integrates and accepts data from the CDRH Electronic Submission Processing (CeSub) system and the CDRH Center Tracking System (CTS) both of which have their own PIA that can be found on the HHS website. In addition to the regulatory documentation listed above, the PII that is resident within the system is specific to the points of contact for the manufacturers to include - name, work (business) email address, and work (business) phone number (business). Additionally, if the sender elects to include it, the e-mail submissions may also contain additional contact information as part of their signature block in the body of the e-mail. This voluntarily submitted information may include job title, work mailing address, and/or work phone and fax numbers. PII contained in submissions is maintained, queried, viewable and download-able to authorize users of CIMS via the following components: I2K+, DocMan, DEEEPS, eService, Postmarket 522 Upload, DEEEPS and Documentum Services. CIMS is only accessible to internal FDA employees and Direct Contractors with an active Personal Identity Verification (PIV) card for Single Sign On (SSO). CIMS also queries a Lightweight Directory Access Protocol (LDAP) server in order to access and retrieve the following forms of PII data: business name, business email and business phone number only. However, none of these data components are stored in CIMS. Finally, there is no PII information collected, maintained, or shared for the following components of CIMS: I2K SOLR, I2K Download, and eBackend. Users of CIMS who access or use the system do not use any personal identifiers to retrieve records held in the system.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	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 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.	Employees/HHS Direct Contractors Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100,000 – 999,999
PIA 25:	For what primary purpose is the PII used?	FDA employees and Direct Contractors use the PII in CIMS to process and correspond with the submitters (industry points of contact) regarding their submissions (supporting documentation; design documents, user manuals, etc.) to the FDA.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	FDA makes no secondary use of the PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	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. 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 at 21 CFR 803, 803.32, and 803.40; 21 U.S.C. 352, 360, 360i, 360j, 371, 174. The Radiological Health regulations at 21 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.
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?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	OMB No. 0910-0120, expires 07/31/2026 (510(k)) OMB No. 0910-0291, expires 06/30/2025 (MedWatch FDA Medical Product Reporting Program) OMB No. 0910-0769, expires 11/30/2026 OMB No. 0910-0025, expires 02/28/2026 (Reporting and Record keeping for Electronic Products)
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.	Consumers making reports of adverse events do not have to provide their PII at all; the submission of their PII is completely voluntary. However, regulated entities are required to provide the work contact information of a point of contact (POC). This can be the PII of any individual authorized to send and receive communications on behalf of the regulated entity and the POC can be changed.
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 FDA's privacy practices change or FDA changes its collection, use, or sharing of PII data in this 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. Note that the system will not share or disclose PII. It will simply store this information as received from regulated industry. Additionally, as regulations change mandating the collection of PII information, there is an open period where the public can submit comments on the regulation.

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 who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have many avenues available for assistance. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), Cybersecurity 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). HHS and FDA policy obligates all permanent and Direct Contractor personnel to report suspected breaches. Within FDA, all suspected breaches must be reported to the Cybersecurity Infrastructure Operations Coordination Center (CIOCC).
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.	All PII is solicited using approved forms and is relevant to facilitate communication between CDRH and regulated organizations. In support of PII integrity and accuracy, CDRH reviews industry submissions on a quarterly basis, and evaluates them to determine whether they are consistent with previous submissions as well as public information. Data integrity and accuracy are important to the extent that PII permits communication with regulated organizations; industry organizations can supply the name of any individual who can communicate with FDA on behalf of the organization. PII relevancy is ensured by the design of the system to collect only the PII that is necessary for authorized uses. Integrity, as well as availability, are both protected by security controls selected per the risk level of the system and consistently with federal guidance from the Office of Management and Budget (OMB) and the National Institutes of Standards and Technology (NIST).
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: Reviewers that need to contact industry submitters for submission review purposes. Administrators: Routine system administration. The administrators are Direct Contractors. Developers: Developers are retained to perform system development data clean up, modifications and integrations as needed. Contractors: The application system administrators are Direct Contractors, and the infrastructure administration is a third-party vendor (ICT21 FDA Data Center and Infrastructure Support Contractor – DXC Technology).
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	System access requests are reviewed and approved by the system/business owner along with the CIMS management team. System accounts are reviewed on a regularly basis to determine if access is still required for each user. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access).
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.	When accounts are created, supervisors indicate 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 and 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 personnel complete mandatory security and privacy awareness training at a minimum of once a year. In addition, all users must accept the HHS Rules of Behavior prior to using the application. Administrators receive training on the CIMS before receiving elevated privileges.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Not applicable (N/A).

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. Schedules that apply to the various records in the system include NARA citation N1-088-08-1, Items 2.1-2.5; General Records Schedule 20, item 2a4; and FDA file codes in the 2000-2700 family. These 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. The CDRH records retention file codes for these specific files are: File Code 2300, Investigational and Pre-Investigational Device Exemptions (IDEs and PIDs), National Archives and Records Administration (NARA) Citation N1-088-08-1, Item 2.3; FDA File Code 2400, Premarket Approval Applications (PMAs), NARA Citation #N1-088-08-1, Item 2.4; File Code 2500, Premarket Notification (510(k)), NARA Citation # N1-088-08-1, Item 2.5. Both File Codes 2300 and 2500 are temporary and records are destroyed when no longer needed, or after 20 years, whichever is later. File Code 2400 is temporary, and records are destroyed when no longer needed, or after 30 years, whichever is later.
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 multi-factor authentication, use of secure sockets layer (SSL) and others. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, require Personal Identity Verification (PIV) cards 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:**	4/4/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	4/7/2025
SOP Review Comments:		**# of Days - SOP Review:**	3

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	4/14/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 4/14/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	7

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	4/14/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
4/14/2025 12:41 PM	BLAND, CRYSTAL	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	4/9/2025	Per FDA's Email, • 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 *10/12/2022*. • 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.	
PTA 05	VILLAFUERTE, NESTOR	4/10/2025	Please write out NARA on the first instance.	