PTA / PIA: FDA - CeSub - QTR2 - 2025 - FDA4918372

Created Date: 4/17/2025 12:50 PM Last Updated: 4/24/2025 4:51 PM

General Information

PTA / PIA Name:	FDA - CeSub - QTR2 - 2025 - FDA4918372	**PTA / PIA ID:**	3034059
Component Name:	FDA - CDRH Center Electronic Submissions	**ATO Boundary Name:**	CDRH Regulatory Review
Overall Status:	Complete	**# of Days - Open:**	7
Submitter:		**Submit Date:**	4/21/2025
Next Assessment Date:	04/23/2028	**Expiration Date:**	4/23/2028
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	Hitesh Doshi
PTA 01A:	POC Title and Organization	POC Title: IT Project Manager POC Organization: OO/OIMT/OTD/DAS/MPB/CDRH
PTA 01B:	POC Email Address	hitesh.doshi@fda.hhs.gov
PTA 01C:	POC Phone Number	240-506-3835
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 System for Uniform Surveillance Pharmacovigilance Report Intake Managed Output (SUS PRIMO) application of the Center for Devices and Radiological Health (CDRH) Center Electronic Submissions (CeSub) component was deactivated since the last PIA.
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 primary purpose of Center for Devices and Radiological health (CDRH) Electronic Submissions (CeSub) is to support the submission, management, and review of required documents for the regulation of the safety and effectiveness of a wide range of medical devices. CeSub enables CDRH to monitor workload, receive electronic submissions, perform the conversion of hard copy submissions to electronic format, manage the submissions repository, and otherwise accomplish regulatory and business functions. Electronic submissions are transmitted via the Food and Drug Administration (FDA)'s separate Electronic Submission Gateway (ESG) system (other submissions are made via regular mail) and once received are internally uploaded into CeSub. FDA maintains a separate PIA for the ESG system. All webpages used by the components of CeSub are nonpublic facing; they are internal only and are accessed by personnel via the FDA's intranet. CeSub is comprised of the following applications: eLoader/eCopies/HTML2PDF, Electronic Medical Device Reporting (eMDR), Facilities Management (FM), Radiological Health Assembler (RH Assembler), and Radiological Health Processor (RH Pro).

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.	Data within the CeSub Image 2000 Repository may include the submitter's name and contact information such as email address, mailing address, and phone number. The eCopies/eLoader/HTML2PDF application collects the following PII: first name, last name, mailing address, phone number, and fax number of the reporter which is normally a manufacturer/industry point of contact (POC) or a third-party representative. The PII is not shared with any system or organization. eCopies/eLoader/HTML2PDF does not collect any non-PII information. The eMDR application captures the following PII that is required in FDA form 3500A: first name, last name, date of birth (DOB) of the patient when available, phone number, fax number, address, email address of the facility where the event occurred, and reporter (industry reporter external to the FDA which is normally a manufacturer or third-party representative) of the event. The form also collects the race, ethnicity of the patient when available. The FM system used by RHPro collects mailing address, phone number, and fax number of the facility. The FM application does not collect any non PII. The collected PII is not shared with any system or organization. For all the CeSub applications usernames are collected and stored in the system. However, because the system utilizes Single Sign On (SSO), user passwords are not stored in the system.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Username

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 Medical Device Amendments to the Food Drug and Cosmetic Act, require manufacturers of medical devices to submit applications to the FDA for approval to ensure that these products are safe, effective, and labeled properly before they become available on the market. Depending on the regulatory class of the device, various types of premarket submissions are submitted. CeSub is an overarching vehicle which contains all of the applications that make up the CeSub system: eLoader, eCopies, HTML2PDF; eMDR; FM; RH Assembler; and RHPro. The information contained in CeSub represents the official record of submissions from manufacturers, including 510K, PMAs, IDEs, labeling data, medical device reporting, and establishment registration and medical device listing forms. All submissions received by CeSub from industry (which contain PII) are submitted either via the ESG or via regular mail. The submissions are then loaded into a staging area. eMDR is used for eMDR submissions and eLoader is used for all other submissions that monitors the staging area to which validate and load those electronic submissions from the staging area into the correct component database and into the Documentum repository. During the loading process, if an error occurs during the validation process, eMDR or eLoader (depending on the submission type as mentioned above) will roll back all transactions within that submission. If there is no error message in the loading process, the application commits all transactions at the end of each submission. Users are notified of a successful or failed load status. For eCopies the administrator is sent an email. For eMDR and RH Assembler, an acknowledgment is sent to the user through the ESG. For RHPro, an acknowledgment is sent via email to the user. Users of the CeSub system consists of FDA employees and Direct Contractors. For all the CeSub applications, usernames are collected and stored in the system. However, because the system utilizes SSO, user passwords are not stored on 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 Date of Birth 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.	Race, ethnicity of the patient when available.
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?	The primary purpose of the Personally Identifiable Information (PII) in Center for Electronic Submissions (CeSub) as a whole is to process submissions and if/when needed, contact the respective industry submitters. The purpose of the PII data in eLoader/eCopies/HTML2PDF is to receive information via these submissions that is voluntary and is used to process the submissions and contact the submitter when required. Information received via Electronic Medical Device Reports (eMDR), FM, Radiological Health (RH), and (Radiological Health Processor (RHPRO) are all industry submissions that are voluntary and are used to process the submissions itself and contact the submitter when required.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	Not applicable - there are no secondary uses for which PII will be used.
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, Sections 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, sections 352, 360, 360hh-ss, 360i, 360j, 371, 374 , 42 U.S.C. 263b-n.
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 In-person Hard Copy Mail/Fax 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. 0910-0291, Expires 06/30/2025 OMB No. 0910-0308, Expires 09/30/2027 OMB No. 0910-0120 Expires 07/31/2026 OMB No. 0910-0025 Expires 02/28/2026
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Submitters of marketing applications receive notice of privacy policies as they are displayed on the submission forms on fda.gov. The submitters are fully aware that they have to submit the PII information in order to successfully process the submission. The information provided in this fda.gov location includes submission processes, a link to the FDA website and privacy policy, and reference to the relevant statute, published regulations and related Federal Register notices. The collection of the information is required per the regulations. Adverse event reporting forms also provide voluntary submitters an opportunity to indicate that FDA may not disclose their identity to device manufacturers. FDA personnel are provided notice at the time of hire of the use and creation of PII about them in the context of their work for the Agency. At network and/or system logon personnel must view and acknowledge a warning message advising against the expectation of privacy when using government systems and resources. For PII obtained from other systems, those systems provide individuals notice. This PIA provides further notice to individuals.

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 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. Additionally, as regulations changes 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.	There is no complaint process specific to CeSub. However, individuals may contact FDA / Center for Devices and Radiological Health (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 CeSub submissions. Additionally, individuals may contact the FDA Privacy Office by using the contact information provided on FDA.gov as well as the FDA intranet. FDA personnel and system users are required to rapidly report actual or suspected PII exposure or compromise (breach) events. 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.
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 CeSub submission process. The submitter is responsible for providing accurate information. Accuracy is ensured by the submitter at the time of reporting. Submitters may correct/update their information themselves and by sending an updated submission (via US Postal Mail, Fax, and/or Compact Disc / Digital Video Disc [CD/DVD]). Integrity and availability are protected by security controls selected and implemented as part of the Authority-to-Operate (ATO) process. Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. CDRH performs semi-annual reviews to evaluate user access. One of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements.
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 CeSub submission process. The submitter is responsible for providing accurate information. Developers: Developers are Direct Contractors who will assist in the development of the system. Contractors: The developers are Direct Contractors. Both regular and privileged users can be Direct Contractors.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to CeSub is based on role-based access control (RBAC), need-to-know and least privilege. The system maintenance team utilizes a "need to know" policy for granting access to the PII information. Typically, only developers, lead analysts, and privileged users are allowed access to this information either through the Web application interface or through the database. For developers and lead analysts the system supervisor determines who receives access. For privileged users, CDRH business supervisors determine which individuals are permitted 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.	All authorized system users require access to this information to perform their job. For the Web application interfaces, there are various user roles for the applications where minimum access rules can be applied. For developers and lead analysts, the system supervisor determines who may have access by reviewing the internal 3530-form submitted by each user to justify access requests.
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 IT security and privacy training annually. A portion of this training is dedicated to the protection and handling of PII overall for the agency. Additional training is available from the FDA Privacy Office.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	None.

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).	CDRH maintains records in CeSub under (1) the National Archives Records Administration (NARA) citation N1-088-08-1, items 2.1-2.5 which includes Premarket Notifications (510(k)) submitted to the FDA to demonstrate that a device is substantially equivalent to a legally marketed device that is not subject to Premarket Approval (PMA). (2) General Records Schedule (GRS) 3.2. Information Systems Security Records; Item 030, System access records. Systems not requiring special accountability for access. Disposition Authority: DAA-GRS-2013-0006-0003. Disposition Instruction: Temporary. Destroy when business use ceases. FDA File Code 2310, Database Records; Data input from or about incoming and outgoing documents submitted or created as part of the review process. Includes information about the initial application and supplements/amendments such as document types, review assignments, status of applications and reviews, dates initiated and completed, and other related information. The disposition: TEMPORARY. Cut off at the end of the calendar year when final action occurs. Destroy/delete 30 years after cutoff or when no longer needed for reference or research, whichever is later. (3) General Records Schedule (GRS) 5.2 Transitory and Intermediary Records; Item 20, Intermediary Records. Disposition: TEMPORARY. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later. Disposition authority DAA-GRS-2022-0009-0002. (4) General Records Schedule (GRS) 3.1 General Technology Records. item 51. Data administration records. All documentation for temporary electronic records and documentation not necessary for preservation of permanent records. Disposition: Temporary. Destroy 5 years after the project/activity/ transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use. Disposition authority: DAA-GRS 2013-0005-0003.

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 role-based 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 for CeSub include role-based access settings, firewalls, Single Sign On (SSO), and (Personal Identity Verification) PIV cards. All the CeSub applications are internal only applications and are SSO enabled. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	4/21/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	4/22/2025
SOP Review Comments:	The FDA's Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls.	**# of Days - SOP Review:**	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	4/23/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 4/23/2025 All comments were addressed, this PIA is ready for SAOP review and approval. 4/21/2025 Please see comments and update accordingly. PIA-22: Per PTA-5, the eMDR application captures the following PII that is required in FDA form 3500A: date of birth (DOB) of the patient when available, race, ethnicity of the patient when available that are not listed as PII elements being collected. PIA-44: Please be advise that GRS 20 no longer exist and was superseded by GRS 4.3 which was superseded in July 2017 by GRS 5.1 and 5.2. Please review the GRS 5.1 and 5.2.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	4/24/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	1

SAOP Signature

Date	User	Type	Name	Original Value	New Value
4/24/2025 12:19 PM	GUENTHER, BRIDGET	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	VILLAFUERTE, NESTOR	4/18/2025	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.”	
PIA 44	BLAND, CRYSTAL	4/21/2025	Please be advise that GRS 20 no longer exist and was superseded by GRS 4.3 which was superseded in July 2017 by GRS 5.1 and 5.2. Please review the GRS 5.1 and 5.2 and update accordingly.	
PIA 22	BLAND, CRYSTAL	4/21/2025	Per PTA-5, the eMDR application captures the following PII that is required in FDA form 3500A: date of birth (DOB) of the patient when available, race, ethnicity of the patient when available that are not listed as PII elements being collected. Please update accordingly.	