

Date Signed: 4/14/2022

Acronyms

ATO - Authorization to Operate
 CAC - Common Access Card
 FISMA - Federal Information Security Management Act
 ISA - Information Sharing Agreement
 HHS - Department of Health and Human Services
 MOU - Memorandum of Understanding
 NARA - National Archives and Record Administration
 OMB - Office of Management and Budget
 PIA - Privacy Impact Assessment
 PII - Personally Identifiable Information
 POC - Point of Contact
 PTA - Privacy Threshold Assessment
 SORN - System of Records Notice
 SSN - Social Security Number
 URL - Uniform Resource Locator

General Information

Status:	Approved	PIA ID:	1429173
PIA Name:	FDA - CeSub - QTR1 - 2022 - FDA2034596	Title:	FDA - CDRH Regulatory Review
OpDIV:	FDA		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	No
PTA - 2:	Does the system include a website or online application?	No
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Agency
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5B:	If no, Planned Date of ATO	11/19/2020
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	No changes since last PIA approval.
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	The primary purpose of 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 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 components:

eLoader/eCopies/HTML2PDF, Electronic Medical Device Reporting (eMDR), Facilities Management (FM), Radiological Health Assembler (RH Assembler), Radiological Health Processor (RH Pro), and System for Uniform Surveillance Pharmacovigilance Report Intake Managed Output (SUS PRIMO).

For info on each of the CeSub components, please refer to the attached CDRH CeSub PIA titled, "CDRH Center Electronic Submissions System (CeSub) PIA 1-25-2022cpc"

PTA - 9:

List and/or describe all the types of information that are collected (into), maintained, and/or shared in 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.

eCopies/eLoader/HTML2PDF 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 PII data is used in the PRIMO application within the SUS component but is not shared with any other system or organization.

The FM system used by RHPPro 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 additional information on CeSub components, please see attached MS Word version of CDRH CeSub PIA, "CDRH Center Electronic Submissions System (CeSub) PIA 1-25-2022cpc."

For all the CeSub subcomponents 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 -9A:

Are user credentials used to access the system?

Yes

PTA - 10:

Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should 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 subcomponents that make up the CeSub system: eLoader, eCopies, HTML2PDF; eMDR; FM; RH Assembler; and RHPPro. 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 RHPPro, an acknowledgment is sent via email to the user.

All SUS/PRIMO electronic and paper submissions which are loaded into eMDR system are reviewed by the reviewers and will be redacted. Once



the redaction of the report is complete, the data is copied from eMDR system to PRIMO system and will be available for reviewers to review the data and push it to the public Manufacturer and User Device Experience (MAUDE).

Users of the CeSub system consists of FDA employees and Direct Contractors. For all the CeSub subcomponents, usernames are collected and stored in the system. However, because the system utilizes SSO, user passwords are not stored on the system.

PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	No
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes
PIA		
PIA - 1:	Indicate the type of PII that the system will collect or maintain	<p>Name</p> <p>E-Mail Address</p> <p>Phone numbers</p> <p>Mailing Address</p> <p>Others - Usernames for all CeSub components Voluntary or mandatory adverse event report submitters may choose to include other PII in the narrative text fields of a report.</p>
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	<p>Employees/ HHS Direct Contractors</p> <p>Public Citizens</p> <p>Other</p>
PIA - 4:	For what primary purpose is the PII used?	<p>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.</p> <p>Information received via Electronic Medical Device Reports (eMDR), FM, Radiological Health (RH), (Radiological Health Processor (RHPRO) and System for Uniform Surveillance (SUS)/Pharmacovigilance Report Intake and Managed Output (PRIMO) are all industry submissions that are voluntary and are used to process the submissions itself and contact the submitter when required.</p>
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	<p>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.</p> <p>Mammography Quality Standards Act Regulations (MQSA), 42 U.S.C. 263b.</p> <p>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.</p>

PIA - 9:	Identify the sources of PII in the system	<p>Directly from an individual about whom the information pertains</p> <ul style="list-style-type: none"> Hard Copy Mail/Fax Online Other <p>Government Sources</p> <ul style="list-style-type: none"> Within the OPDIV <p>Non-Government Sources</p> <ul style="list-style-type: none"> Members of the Public Private Sector
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	<p>OMB No. 0910-0291, Expires 01/31/2025</p> <p>OMB No. 0910-0308, Expires 4/30/2024</p> <p>OMB No. 0910-0120 Expires 6/30/2023</p> <p>OMB No. 0910-0025 Expires 8/31/2023</p>
PIA - 9B:	Identify the OMB information collection expiration date.	6/30/2023
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	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 must 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.

Voluntary

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 submitting of records to the FDA. However, there is no opt-out option for users as the PII data in the reports is required for submission processing per FDA regulations. FDA personnel whose PII is in the system may not opt out and continue to perform their duties involving use of the system; opting out renders them unable to use the system.

PIA - 12: Is the submission of PII by individuals voluntary or mandatory?

PIA - 13: Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason

<p>PIA - 14:</p>	<p>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). Alternatively, describe why they cannot be notified or have their consent obtained</p>	<p>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.</p>
<p>PIA - 15:</p>	<p>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</p>	<p>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.</p> <p>FDA personnel and system users are required to rapidly report actual or suspected PII exposure or compromise (breach) events.</p> <p>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.</p>
<p>PIA - 16:</p>	<p>Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not</p>	<p>PII is provided voluntarily by the submitter in order to complete the CeSub submission process. The</p>

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 - 17:

Identify who will have access to the PII in the system and the reason why they require access

Users
 Developers
 Contractors

PIA - 17A:

Provide the reason of access for each of the groups identified in PIA -17

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 - 17B:

Select the type of contractor

HHS/OpDiv Direct Contractor

PIA - 18:

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 - 19:	Describe the technical methods in place to allow those with access to PII to only access 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 - 20:	Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system 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 - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	None.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s)	CDRH maintains records in CeSub under (1) then 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) 20, item 2a4, which calls for maintaining records with a temporary disposition with the cutoff at the end of the calendar year after final action is completed or product is withdrawn from the market and under which records are deleted/destroyed when they are no longer needed for business and regulatory purposes, or 20 years after the cutoff date, whichever is later; and (3) FDA file codes in the 2000-2700 family, which typically call for deletion of records when no longer needed for business and regulatory purposes, or after 20 or in some cases 30 years, whichever is later.

PIA - 24:

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.