Privacy Impact Assessment (PIA): FDA - RMS - QTR1 - 2023 - FDA2077771

Date Signed: 2/6/2023

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:**	1603669
PIA Name:	FDA - RMS - QTR1 - 2023 - FDA2077771	**Title:**	NCTR Research Management System
OpDiv:	FDA		

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The iRIS application has been removed from the system and website (NLaunch.fda.gov) is now used to manage access to the individual modules within RMS.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	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 purpose of the Research Management System (RMS) is to provide the essential

		tools for gathering data and for providing the necessary decision support mechanisms used to allocate available resources to new and ongoing research efforts. It is used by the NCTR management to plan and monitor research and ensure efficient use of NCTR resources. It provides tools for NCTR Office of Research and Office of Management to enable proper planning of research projects and conduct activity-based management of personnel, laboratory equipment, supplies, facilities, and animals. RMS is an information technology (IT) resource which supports NCTR's Strategic Research activities in knowledge-based, method-driven, agent-driven, concept-driven and new strategies for the prediction of toxicology research areas. System "users" consist of individuals participating in the management of research at NCTR. All users who currently have or will have access to RMS will be internal to NCTR. There are no external users. Access to individual modules of RMS is requested through the NCTR User Account Request form.
PTA - 5:	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.	The RMS collects data required for NCTR research protocol approval and tracking

		efforts as well as data needed to conduct activity-based cost analysis functions. The types of non-PII data collected for these functions include protocol review and approval information, document production and publishing, cost factors, training requirements, and full-time equivalent (FTE) availability and resource (labor hour and dollar) costs estimated for and consumed in support of specific projects (e.g., protocol approval and tracking). RMS collects the following personally identifiable information (PII): (a) first and last names and email addresses of FDA employees and Direct Contractors who are authors or co-authors of published articles listed within the system; (b) names and email addresses of non-FDA personnel credited as co-authors of listed articles (these are scientists who willingly and knowingly contribute to scientific research in anticipation of publication); (c) phone number; (d) education of authors and co-authors.
PTA - 5A:	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. The system providing credentials is
PTA - 6:	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 Research Management System (RMS) software provides high quality research management. It contains software that provides functions such as: project planning, decision support, management of animal utilization, employee time collection, laboratory and environmentally controlled area usage, animal dietary requirements and tracking of other resource usage required for toxicological and regulatory research. FDA uses the data collected within RMS components to ensure agency resources are employed to perform research that supports FDA's ability to make science-based regulatory decisions. No regulatory data is collected or stored in RMS.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No

PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
PTA - 9:	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.	Only FDA/NCTR staff have access to the website and are authenticated using a PIV card. The website serves as an access management for RMS modules. The users (Government full time equivalent (FTE's) and Direct Contractors) have access only to the applications and data comprising RMS for which they have a business need based on their role.
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:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Email Address Education Records Name Phone numbers Other - Free text Field - The selection of education records may be specific to the type of degree (i.e., PhD, Master's Degree, etc.) and university attended.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	The purpose of PII collection is to track resources and work, and, to associate research manuscripts with authors (along with their institution affiliation) and give them credit for their work (manuscript and author is publicly available information).
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	No secondary uses.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	21 U.S.C. 301 (Federal Food, Drug and

		Cosmetic Act), 5 U.S.C. 301 and 21 U.S.C. 393 (general authority to prescribe procedures and use of information and records).
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	First and Last Name(s)
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Email Government Sources Within the OPDIV Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
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	Submission of PII is voluntary as the term is defined under the Privacy Act. There is no dedicated opt-out process. Authors and co-authors willingly provide their PII for contact purposes and in order to be associated with their research and related publication(s). In addition, if the required information is not provided, the individual may not be allowed to participate in a research protocol in which animals are involved.
PIA - 14:	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.	Authors of scientific manuscripts willingly attach their name to the published articles listed in the system. If the agency changes the collection, use, or sharing of PII data in this system, the affected individuals (both agency personnel and external authors) will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on an FDA web site or email notice to the individuals.
PIA - 15:	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	Individuals may raise any concerns by contacting NCTR/FDA via phone, email or

	exists, explain why not.	mail information provided on FDA.gov. FDA authors may self-correct errors related to their PII (e.g., spelling of name) and may also address concerns through several available channels including FDA's Employee Resource and Information Center (ERIC), IT Security, the Privacy Office, and their office management. Where inaccuracies result from the article publisher (journal publisher), authors may contact the publisher directly.
PIA - 16:	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.	Personnel are responsible for maintaining accurate work contact information and if needed may use internal processes to update or correct inaccuracies in their work contact information. Information may also be corrected if errors are identified during the quarterly review of system access permissions. Where inaccuracies result from the article publisher (journal publisher), authors may contact the publisher directly.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	USERS: FDA employees (including Direct Contractors) access and analyze data in the system in the performance of duties. Some of the RMS users are Direct Contractors. ADMINISTRATORS: Manage the system and associated workflow; control access. DEVELOPERS: Maintain and update the software/database as needed to ensure applications are operational. CONTRACTORS: To review research protocols and determine level of effort required/expended by the contractor in support of the research.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users who require access to the information system are NCTR staff and they must have supervisor approval and signature confirming their need for access before access is granted.
PIA - 20:	Describe the technical methods in place to allow those with access	The user's supervisor will establish the

	to PII to only access the minimum amount of information necessary to perform their job.	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 during which time users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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.	All personnel are required to complete FDA's security and privacy awareness training at least annually. Completion of training is tracked by the Office of Digital Transformation (ODT).
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users are instructed on the proper system use by research division staff and/or management staff. A user guide is available.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	RMS database records are retained/destroyed under FDA file code 4200, and National Archives & Records Administration (NARA) approved citation N1-088-07-001. This covers data fields supporting various applications such as project planning, protocol tracking, pathology tracking for animal utilization and animal dietary requirements, laboratory and environmentally controlled area usage, employee and contractor tasks and approvals, procurement tracking, document tracking, personnel data and other related information. The above records control schedules specify disposition is temporary and direct disposition as authorized under relevant subject records series for information in data fields. If data is used to support other projects or modules within RMS, it may be deleted after the completion of the project or the deletion of this module or 15 years after the research experiment is completed, whichever is shortest.
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 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 use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. This information system is installed on servers located in FDA Data Centers, which have physical security controls in place.

Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls.

Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.