Privacy Impact Assessment (PIA): FDA - GM - QTR4 - 2020 - FDA1851023

Date Signed: 10/7/2021

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:**	1290173
PIA Name:	FDA - GM - QTR4 - 2020 - FDA1851023	**Title:**	FDA - OC Administrative Applications
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	11/15/2019
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	A new module (Operations) has been released for use in association with the Office of Orphan Products Development (OOPD) application and is addressed in this Privacy Impact Assessment (PIA).
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 Administrative Applications Authority to Operate (ATO) consists of many applications and components. This PIA covers seven related

		applications within two Food and Drug Administration (FDA) offices: The Office of Women's Health (OWH), and The Office of Orphan Products Development (OOPD). The specific applications covered in this PIA are OWH Grants Management, OWH Outreach Activities, OOPD Grants and Applications, OOPD Natural History Grants, OOPD Designations, OOPD Pediatric Device Consortia and OOPD Operations. The purposes of these systems are to support the missions of OOPD and OWH. These systems were grouped together to be addressed in a single document on the grounds that they are used to conduct similar activities and are governed by many of the same authorities (systems of records notices; legal authorities to collect; retention schedules). The mission of the OWH is to protect and advance the health of women through policy, science, and outreach and to advocate for the participation of women in clinical trials and for sex, gender, and subpopulation analyses. OWH achieves its mission by supporting scientific research and collaborating with other government agencies and national organizations to sponsor scientific and consumer outreach efforts. OWH Grants Management (GM) is used to manage grants awarded to product sponsors. The purpose of the OWH Outreach Activities application is to document OWH's success in conducting outreach and meeting its mission. When stakeholders elect to make use of OWH outreach materials, notations may be added in the system regarding when and where these will be used.
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.	OWH GM and OWH Outreach Activities applications collects the following PII information: phone number, email address, mailing address, fax number, social media contact information (handles), and first and last name. None of the OOPD applications or OWH applications are subject to the Privacy Act and do not use personal identifiers to retrieve records from 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	For OWH Grants Management collected documents and information may include the contact information for a point of contact (names,

		addresses, e-mails, phone numbers, fax numbers, social media contact information), and information concerning proposed projects and research including methods, budgets, needed resources and materials, and records of progress and outcomes. The application currently does not contain personal background information about scientific researchers such as resumes or curricula vitae (CVs) of researchers (e.g., containing contact information, education, work, and other relevant history). The OWH Outreach Activities application is used to record assignments or tasks related to outreach, which may include promotional materials, schedules, or agendas of events, contact information for stakeholders or collaborators (names, addresses, e-mails, phone numbers, fax numbers, social media contact information), and communications among FDA staff or others related to planning events. The purpose of the application is to document OWH's success in conducting outreach and meeting its mission. When stakeholders elect to make use of OWH outreach materials, notations may be added in the application regarding when and where these will be used. Personally identifiable information (PII) may be incidentally included in communications, for example, if FDA staff communicate with external stakeholders and the communications are retained in the system. The two OWH applications operate using a single-sign-on process to control access and do not store usernames or passwords.
PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	Yes
PTA - 10B:	Please specify which PII data elements are used.	For OWH Grants Management collected

		documents and information may include the contact information for a point of contact (names, addresses, e-mails, phone numbers, fax numbers, social media contact information), and information concerning proposed projects and research including methods, budgets, needed resources and materials, and records of progress and outcomes. The application currently does not contain personal background information about scientific researchers such as resumes or curricula vitae (CVs) of researchers (e.g., containing contact information, education, work, and other relevant history). The OWH Outreach Activities application is used to record assignments or tasks related to outreach, which may include promotional materials, schedules, or agendas of events, contact information for stakeholders or collaborators (names, addresses, e-mails, phone numbers, fax numbers, social media contact information), and communications among FDA staff or others related to planning events. The purpose of the application is to document OWH's success in conducting outreach and meeting its mission. When stakeholders elect to make use of OWH outreach materials, notations may be added in the application regarding when and where these will be used. Personally identifiable information (PII) may be incidentally included in communications, for example, if FDA staff communicate with external stakeholders and the communications are retained in the system.
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	Name E-Mail Address Phone numbers Certificates Date of Birth Mailing Address Others - OWH Outreach may contain point of contact information for stakeholders and collaborators as well as incidental PII contained in copies of communications. The collected contact information is personal contact information. Both Grants Management systems may include contact information for points of contact and researchers. Neither Grants Management systems contain resumes or CVs of applicants, but either may do so in the future.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Business Partners/Contacts (Federal, state, local agencies)

		Employees/ HHS Direct Contractors Public Citizens Other - Grant recipient points of contact, OWH stakeholders and customers. "Employees" includes Direct Contractors.
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Above 2000
PIA - 4:	For what primary purpose is the PII used?	The primary purposes of use for the PII: Coordinate efforts of staff; coordinate evaluation of grants (OOPD); assist in project management oversight of grants; document activities and accomplishments; and assess progress and outcomes of grant activities. For Operations, the PII is collected for the purpose of device/administrative tracking of FDA issued devices.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	None.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	The Federal Food, Drug, and Cosmetic Act (FFD&CA), 21 U.S.C. 399(b), 399ee, and 399bb(c). OWH Outreach: The FFD&CA provides that the Director of the Office of Women's Health will "(3) provide information to women and health care providers on those areas in which differences between men and women exist; [and] (4) consult with pharmaceutical, biologics, and device manufacturers, health professionals with expertise in women's issues, consumer organizations, and women's health professionals on Administration policy with regard to women." 21 U.S.C. 399(b). This system is used to document OWH's efforts to meet this mandate. It may capture PII incidentally. OWH Grants Management: Section 399(b) further provides that the Director OWH will "establish short-range and long-range goals and objectives within the Administration for issues of particular concern to women's health within the jurisdiction of the Administration, including, where relevant and appropriate, adequate inclusion of women and analysis of data by sex in Administration protocols and policies." Grants are provided in furtherance of this requirement.
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Email Online Government Sources Within the OPDIV Other HHS OPDIV

		Non-Government Sources Members of the Public Private Sector
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	No specific prior notice is provided. Applicants voluntarily submit applications and related information and are thereby aware of the PII or other information they choose to submit. Information is either submitted by the subject individuals themselves (as noted above, e.g., in the case of the Grants Management applications); concerns employees who are aware that information about their activities will be known to their employers; or is a record of communications with members of the public. Regarding OOPD Grants and Applications, the NIH would address providing notice to individuals whose data is collected in the data file NIH provides to FDA as noted elsewhere in this assessment. FDA personnel (permanent employees, direct contractors, fellows, etc.) are notified at the time of hire and consent to the submission and use of their personal information as a condition of employment. HHS and FDA Center Representatives, and the various individuals involved with the specific data collection and use provide notification to personnel at the time the data is requested. This PIA provides further notice.
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	For grants applicants, applicant organizations choose to submit information in order to apply for grants. Individual PII is limited to points of contact and individuals that may participate in grants activities. Submission is voluntary; individuals and organizations may opt not to apply or submit information. Some PII about members of the public may be maintained in the OWH Outreach application. This information will concern collaborations with stakeholder groups or individuals. Members of the public can exercise control over PII they include in communications with FDA. PII retained will concern activities conducted cooperatively and the inclusion of PII will be incidental to this documentation. Some of these systems use employee PII for authentication and access controls. There is no method for employees to opt not to submit PII. Permanent employees, Direct Contractors, fellows, and other personnel must provide their PII in order for the Agency to process administrative materials and securely administer access to Agency information and property.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to	No such major changes are expected. If a major change or use of data were to occur, users would

	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	be notified via individual e-mail, FDA-wide e-mail and/or in updated public documents such as FDA.gov, this PIA, or other publications. If changes were to affect employee information, many other channels may be used to inform them, including phone, e-mail, notices on the FDA intranet, or through supervisors.
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 exists, explain why not	FDA personnel have existing procedures and services available such as FDA's Employee Resources and Information Center (ERIC). External individuals may use any of a number of avenues to raise concerns, including contacting FDA offices through FDA.gov (phone, mail, e-mail) and by using information provided on forms submitted by individuals.
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	External submitters are responsible for the accuracy and relevancy of the information they submit. Information related to external submitters is corrected in the course of use and/or at the request of the individual. Personnel are responsible for providing accurate information and may independently update and correct their information at any time. Information is relevant because it is strictly limited to information needed for access and authentication purposes. For all PII in all of these applications, integrity and availability are protected by security safeguards. Each system has appropriate controls selected based on its level of risk (as categorized under the National Institute of Standards and Technology's (NIST's) Federal Information Processing Standard (FIPS) 199) and NIST's Special Publication 800-53 on Security Controls.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17 Users: For the purposes of this document users are FDA employees. Users require full access to grants applications in order to conduct activities related to the mission of the Office. Administrators: All administrators with access to PII are also application users for those applications and will have access as users. Developers: Developers will not normally have access to PII but may in the course of maintaining the systems or providing technical assistance. Contractors: Some developers may be Direct Contractors and will have access under the same circumstances.	
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	Users who require access to the information system need to have supervisor approval and sign off before access is granted. The user's

		supervisor will use an account creation form to specify the minimum information system access that is required in order for the user to complete his/her job. The Agency reviews the access list for the system on a quarterly basis to review and adjust users' access permissions, and, to remove unnecessary accounts from the system.
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	Management establishes roles for individual personnel, with role-based restrictions permitting access only to information that is required for each individual to perform his/her job.
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	All system users at FDA complete annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity, and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Information Management and Technology (OIMT) verifies that training has been successfully completed.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	Each application within the AdminApps system has user training and user documentation for the system users. Access is restricted through system access control. All users are instructed on adhering to the HHS Rules of Behavior in the context of their work involving this system. For additional privacy guidance, personnel may contact the Agency's Privacy Office. Privacy program materials are available to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA.
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)	For OWH Grants Management, OOPD Grants and Applications, and OOPD Natural History Grants, records are retained under FDA File

		Code 1721, (National Archives Records Administration) (NARA N1-88-04-03), Grants Awarded by FDA. Records are destroyed or deleted seven years after the grant is terminated or after the last payment is made. For applications for grants received but not awarded maintained in OOPD Grants and Applications and OOPD Natural History Grants, records are retained under FDA File Code 1722, (NARA N1-88-04-03), Grants Approved (but not funded) or Disapproved Applications. Records are destroyed or deleted three years after the date of cancellation or the date of competitive review. OWH Outreach, records are retained under FDA File Code 8420, (NARA NC 188-07-02), Program Management Files. The "cutoff date" is after the final action/report for which the record is needed, or at the end of the calendar year in which they are needed. Records are maintained a minimum of three years then destroyed seven years after cutoff date, or when no longer needed for reference, whichever is sooner. OPERATIONS
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. 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 NIST's Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.