US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/12/2016

OPDIV:

FDA

Name:

Administrative Applications

PIA Unique Identifier:

P-5317511-817524

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The FDA collectively employs AdminApps to securely and efficiently operate FDA property, resources, and administrative and reporting systems. This PIA assesses seven specific applications:

The FDA Amendments Act of 2007/FDA Safety and Innovation Act of 2012 Deliverable Tracking System (FDAAA-FDASIA) is used by FDA personnel to track deliverables (work products) mandated by law to ensure that the Agency is fulfilling its responsibilities under this legislation. Work products include annual reports on collecting user fees; providing waivers to expedite approval of certain new drugs; engaging patients and other stakeholders; and increasing protections to the nation's supply chain. Information contained in the system includes statistics on these activities but no PII.

Federal Register (FR) provides the ability for the Agency to track an FR document through its life cycle.

Awards provides the ability for FDA's Incentive Award Officers to track nominations, approval, transactions, and ceremonies related to awards for employee performance, and to create certificates and letters provided to employees and their supervisors.

Office Moves provides the ability for administrative staff to plan and track relocations of offices and divisions within the Agency from one building or part of a building to another.

ePortal is a small application that permits users of the FDA intranet to locate individuals and offices with the FDA. This application contains three components: "Edit My Info" allows an individual to update their phone numbers and office locations, such that other users of ePortal will be able to locate them. "Find FDA Staff" allows an individual to search for individuals (both employee and non-employee) within FDA. Find FDA Staff accesses and uses information retained in Enterprise Administrative Support Environment (EASE), another OC Admin Apps application addressed in another PIA. It returns results on the screen then allows user to either Export to Excel or Print Screen. "Search for FDA Organizations" allows an individual to search for organizations within FDA. It also searches EASE data. It returns results on the screen including organizational structures then allows user to either Export to Excel or Print Screen.

Public Calendar tracks the schedule of public events attended by approximately 25 FDA senior management officials. This information is consulted when staff posts information about their attendance at these events on the FDA.gov Internet site. There is no direct connection, however, between Public Calendar and FDA.gov.

PMAP Rating tracks the annual Performance Management Appraisal Program (PMAP) of all General Schedule (GS) employees in FDA. Primary users are FDA Supervisors, Award Incentive Officers (AIOs), and PMAP Coordinators. The application tracks the completion and receipt of the signed forms from each employee three times a year (Initial, Mid-year, and Final). It tracks the final summary scores, award pool information, award levels and individual amounts, and HHS reporting requirements.

Describe the type of information the system will collect, maintain (store), or share.

AdminApps contains information necessary for the Agency to securely and efficiently operate FDA resources and administrative programs. With the exception of FDAAA-FDASIA, all of the applications addressed in this PIA (FR, Awards, Office Moves, ePortal, Public Calendar, and PMAP Rating) contain work contact-related PII. This PII includes name, work e-mail address, physical address and phone number. FR might also store non-employee PII (e.g., name).

FDA uses the FDAAA-FDASIA application to track and collect status information and changes to work products required by the FDAAA-FDASIA legislation. Access to this application requires a username and password.

FR tracks information relating to notices FDA published in the Federal Register, and related public comments and public administrative records. While commenters are advised that the substance of their comments, including their PII, will be made public, some commenters may choose to include their PII. FR uses single sign on enabled and does not require a username or password.

Awards tracks award name, nominee information (name, organization and grade) and ceremony information. Information in this application is retrieved by name or other unique personal identifier and is therefore subject to the Privacy Act. Access to this application requires a username and password.

Office Moves tracks the mover's name, organization, and new and old office locations. Access to this application requires a username and password.

ePortal does not itself contains PII, but it accesses name, office location, office or division name, e-mail address, and work phone number from EASE. Access to this application is by single sign-on and does not require a username or password.

Public Calendar contains the name, job title, and certain daily activities (attendance at public events) of approximately 25 senior FDA management executives. Access to this application is by single sign-on and does not require a username or password.

PMAP Rating contains the names of FDA employees; whether their PMAP has been completed and signed each time it is due (three times a year: Initial, Mid-year, and Final); final summary evaluation scores; award pool information; award levels and individual amounts, and HHS reporting requirements. Information in this application is retrieved by name or other unique personal identifier and is therefore subject to the Privacy Act. Access to this application is by single sign-on and does not require a username or password.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

This PIA covers seven of the AdminApps applications.
FDAAA and FDASIA expanded FDA's authority and responsibilities to ensure that FDA staff has the resources to conduct the complex and comprehensive reviews necessary to approve new drugs and devices. The FDAAA-FDASIA application manages and tracks the status of deliverables associated with the two laws and the relevant agency responsibilities, authorities, and regulations. This application does not collect or store any PII.

FR tracks the full lifecycle workload of the Federal Register business process for the Agency as mandated by law.

Awards tracks the full lifecycle workload of the awards business process for the Agency. The application tracks award name, nominee information (name, organization and grade) and ceremony information.

Office Moves provides an automated process for tracking office moves of employees throughout the Agency. The application tracks employee name and office address as well as move dates.

FR stores employee contact information (i.e., name, phone number, office and e-mail addresses) that was originally included on the public dockets. Because public docket information may include non-employee PII (such as name or other contact information) that individuals commenting on a public notice have shared as part of their comment, FR may store non-employee PII as listed above.

ePortal is a small application that permits users of the FDA intranet to locate individuals and offices with the FDA. This application contains three components: "Edit My Info" allows an individual to update their phone numbers and office locations, such that other users of ePortal will be able to locate them. "Find FDA Staff" allows an individual to search for individuals (both employee and non-employee) within FDA. Find FDA Staff accesses and uses information retained in Enterprise Administrative Support Environment (EASE), another OC Admin Apps application addressed in another PIA. It returns results on the screen then allows user to either Export to Excel or Print Screen. "Search for FDA Organizations" allows an individual to search for organizations within FDA. It also searches EASE data. It returns results on the screen including organizational structures then allows user to either Export to Excel or Print Screen.

Public Calendar tracks the attendance of approximately 25 senior management officials at public events. This information is retained, and later consulted when posting this information to the FDA.gov Internet site, but there is no direct link between Public Calendar and FDA.gov. Primary users are the Administrative Assistants of the senior management officials. There are approximately 60 users.

PMAP Rating tracks the annual Performance Management Appraisal Program (PMAP) of all General Schedule (GS) employees in FDA. Primary users are FDA Supervisors, Award Incentive Officers (AIOs), and PMAP Coordinators. The application tracks the completion and receipt of the signed forms from each employee three times a year (Initial, Mid-year, and Final). It tracks the final summary scores, award pool information, award levels and individual amounts, and HHS reporting requirements. Primary users are the Administrative Assistance of the officials who are required to report. There are approximately 60 users.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

E-Mail Address

Mailing Address

Phone Numbers

NOTE: The PII checked above is all work contact information for FDA employees.

The Awards Application also tracks nominee information including name, organization and grade. It also provides a unique identifier for each nomination.
User credentials (username and password)

While commenters are discouraged from including sensitive information in the comments they provide to the Federal Register, some may choose to include PII in their response unsolicited.

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

NOTE: Employees includes direct contractors. FR might also maintain non-employee (Public Citizen) PII that individuals commenting on a public notice shared as part of their comment. Such submissions are voluntary and FDA's Federal Register publications inform individuals of the procedures for commenting on a notice and advise submitters that submitted comments are made public.

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The PII is used for internal administrative and reporting activities, personnel management functions, and to maintain the security of Agency IT systems and physical property.

Describe the secondary uses for which the PII will be used.

Not Applicable.

Identify legal authorities governing information use and disclosure specific to the system and program.

The implementation of these applications is authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures of the applications are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

HHS SORN 09-90-0018, Personnel Records in Operating Offices

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

Not Applicable

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

FDA personnel (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. FDA center representatives, and the various individuals involved with the specific data collection and use provide notification to the employees and non-employees at the time the data is requested.

For some applications, external individual submitters (i.e., non-employees) were notified on forms they submitted; these applications are no longer used. Other methods of notification include Federal Register publications (e.g., comment submission guidance and SORNs), privacy statements on FDA.gov and other resources provided on FDA.gov. FDA's Federal Register notices also often inform individuals of the procedures for commenting on a notice and advise that submitted comments may be published in full, including PII and any other information submitters choose to include in their comments.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

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.

There is no method for employees to opt out of submitting their PII. Permanent employees, direct contract employees, 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.

External individuals submitting comments to the Federal Register are not mandated to submit any PII. External individual (non-employees) submitters were notified on forms they submitted (no longer in use), in Federal Register publications (e.g., comment submission guidance and SORNs), privacy statements on the FDA.gov and in other resources provided on FDA.gov. FDA's Federal Register notices inform individuals of the procedures for commenting on a notice and advise that submitted comments may be made public.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

If a major change in the collection, and use or sharing of PII data for these applications occurs, users will be notified via individual e-mail notification, FDA-wide e-mail and/or in updated notice statements on submission forms and Federal Register publications. However, no such changes that would affect the rights or interests of the individuals are anticipated.

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.

FDA personnel may resolve such concerns by contacting the appropriate system administrator, FDA's Employee Resources and Information Center (ERIC) or the Computer Security Incident Response Team (CSIRT). Any changes to an individual's name or address would need to be updated using a Standard Form 50 or 52, which is the process used to make such changes used by all FDA employees, and the data would be updated in the separate human resources information system.

External individuals may use any of a number of avenues to raise concerns, including contacting FDA offices through FDA.gov (phone, mail, mail and by using information provided on forms submitted by individuals. External individuals submitting comments to the Federal Register are not mandated to submit any PII. FDA's Federal Register notices consistently inform individuals of the procedures for commenting on a notice and advise submitters that submitted comments are published in full, including PII and any other information submitters choose to include in their comments.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

FDA relies on its personnel to ensure the accuracy and integrity of the information entered into these applications. FDA personnel are responsible for providing accurate information and may independently update and correct their information at any time.

FDA lacks a reference model to periodically check the integrity and accuracy of the PII of external submitters, but provides avenues to ensure all information is as complete, accurate, timely, and relevant as possible. Information related to external submitters is corrected in the course of use and/or at the request of the individual. External individuals submitting comments to the Federal Register are not mandated to submit any PII. FDA's Federal Register notices consistently inform individuals of the procedures for commenting on a notice and advise submitters that submitted comments are published in full, including PII and any other information submitters choose to include in their comments.

Integrity and availability are protected by the appropriate security controls 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.

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

Users:

Require access to the system in order to assign and track assignment. Note that "users" may include subject individuals, supervisors, or business function administrators.

Administrators:

Administrators may be application administrators who require access to conduct business functions, or application administrators who require access in order to create and manage user accounts for specific applications.

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 as developers.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Users who require access to the application 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 application access that is required in order for the user to complete his/her job. The agency reviews the access list for the application on a quarterly basis to review and adjust users' access permissions, and to remove unnecessary accounts from the application.

Describe the 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.

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 requires all Agency personnel and direct contractors to complete FDA's IT Security and Privacy Awareness training at least once every 12 months. A portion of this training is dedicated to guidance on recognizing and safeguarding PII.

Describe training system users receive (above and beyond general security and privacy awareness training).

Help links are available within applications, and instructional materials are available on the FDA intranet for all applications with the exception of FDAAA-FDASIA.

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 provided to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Office Moves application records are retained under General Records Schedule (GRS) 11, Items 1 and can be destroyed after two years. Awards application records are retained under GRS 10-12a1 and can be destroyed after two years. FR application records are retained under GRS 23-8 and can be destroyed when 2 years old, or 2 years after the date of the latest entry. Records retained under 2631a can be transferred to NARA 30 years after cutoff while those under 2631b can be destroyed 30 years after cutoff. ePortal data is retained under NARA Citation N1-88-04-03, and data is retained only until EASE accepts changes and updates to its data files, and data is superseded and deleted. Public Calendar application records are retained under GRS 23-5 (Schedules of Daily Activities) and will be destroyed or deleted when two years old (see also NARA schedule N1-GRS-87-19 item 5a). PMAP Rating data is retained under GRS 1-23a3, and are destroyed when four years old.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

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 that PII entered via these systems is immediately pulled through the web-based systems into internal systems not connected to the web, removed from the public site, and not accessible to others submitting information via these systems or fda.gov.

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.