US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/12/2016

OPDIV:

FDA

Name:

Administrative Applications: Dockets Repository

PIA Unique Identifier:

P-5312033-388733

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 one specific application, Dockets Repository.

Dockets Repository enables Agency staff to review existing dockets and their associated public comments and administrative files prior to 2009. Dockets Repository data includes FR notices, public comments received, and administrative record documents.

Note that Dockets Repository is no longer used to collect information and is now only used as a repository. When Dockets Repository was in active use, individuals providing public comments to FR did not use Dockets Repository directly, and the application was accessed (for FDA purposes) only by FDA employees. Although other agencies also used Dockets Repository and established processes to make Dockets Repository available to the public, FDA did not. Information in Dockets Repository is not retrieved by name or other unique personal identifier and it is not subject to the Privacy Act.

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.

Dockets Repository contains work contact-related PII. This PII includes name, work e-mail address, physical address and phone number. Dockets Repository might also store non-employee PII (e.g., name). Dockets Repository tracks information relating to notices FDA published in the Federal Register, and related public comments and public administrative records.

Dockets Repository requires access to the FDA network but no system-specific username and password.

Note that public comments originated in the Federal Register, and then this information was moved from there to Dockets Repository and the PII was not submitted directly to either of these applications. Dockets Repository is now an archive of pre-2010 documents only and no new PII is being imported into it.

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

The Dockets Repository application is currently retired and is only used for querying dockets data (e. g., FR notices, public comments received and administrative record documents) prior to 2009.

Dockets Repository 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, these three applications may also store non-employee PII as listed above.

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 maintained is all work contact information.

Some Dockets Repository submissions may include other PII that members of the public have chosen to submit. FDA makes efforts to ensure submitters are aware this information may be made public and discourages the inclusion of sensitive information.

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

Employees

Public Citizens

NOTE: Dockets Repository might also maintain non-employee PII that individuals commenting on a public notice shared as part of their comment. Such submissions are voluntary and FDA's Federal Register publications generally 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 (if any) is submitted unsolicited by individuals make public comments on documents published in the Federal Register.

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?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Online

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 external individuals (non-employees) submitters were notified on forms they submitted (no longer in use); these applications are no longer used. Other methods of notification include Federal Register publications (e.g., comment submission guidance and SORNs), privacy statements on the 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 not to submit PII. Permanent employees, 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 are 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, e-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 Personnel are responsible for providing accurate information and may independently update and correct their information at any time.

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.

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 Dockets Repository.

All users are instructed on adhering to the HHS Rules of Behavior in the context of their work involving these applications. 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.

Dockets Repository records are retained under FDA file codes 2631a (NARA approved citation N1-88-04-2) and 2631b (NARA approved citation N1-88-04-2). Records retained under 2631a can be transferred to NARA 30 years after cutoff while those under 2631b can be destroyed 30 years after cutoff.

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.