US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/12/2016

OPDIV:

FDA

Name:

Administrative Applications: FOIA-Related Applications

PIA Unique Identifier:

P-7642165-814612

The subject of this PIA is which of the following?

Minor Application (child)

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?

Yes

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.

This PIA addresses three applications within the overarching AdminApps system. These applications are: Freedom of Information (FOI); FOI Invoicing; and FOI OnLine Request Submission.

FOI tracks work related to requests under the Freedom of Information Act (FOIA). FOIA permits the public to request information from any federal agency. Unless one of twelve exemptions applies, individuals are entitled to receive any information held by these agencies. FOI enables FDA to monitor the processing of approximately 10,000 FOIA requests the agency receives annually. This application helps track and coordinate the processing of FOIA requests and can also be used to generate reports concerning requests received, responded, and pending, including providing metrics on the time taken to respond to requests.

FOI OnLine Request Submission allows members of the public to submit FOIA requests using a form located on the FDA.gov web page.

FOI Invoicing is used to calculate and track charges made to FOIA requestors. Under FOIA, requestors may be required to pay reasonable standard charges for document search, duplication, and/or review.

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

FOI may contain contact information about requesters, copies of documents related to requests for information and responses, and any other content sent by members of the public along with requests. FOI requires FDA employee users to log on using application-specific credentials. Requestors do not need to use authentication credentials.

FOI Invoicing may contain contact information for FOI requesters (e.g., name, phone numbers, addresses, e-mail addresses) as well as itemized accounts of charges invoiced for services and records of payments received. FOI Invoicing FDA employee users to log on using application-specific credentials. Requestors do not need to use authentication credentials.

FOI OnLine Request Submission is a web-enabled tool. Requests do not reside on this application and are instead transferred to the FOI application after a short period (it collects but does not maintain, store, share, or otherwise come in contact with PII). This application does not require application-specific credentials.

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

FOI may contain contact information of requestors (name, address, phone number, e-mail); copies of requests made (PDF or other); name s of individuals working on researching and responding to such requests; and copies of communications among offices as request responses are assembled. Note that while not requested or expected, many FOIA submissions contain additional information such as the reasons for the request or information about the submitter. Also, requested documents may contain PII. PII will be redacted if releasing it "would constitute a clearly unwarranted invasion of personal privacy." The total number of requests recorded in the application may exceed a half-million. Not all of these records will contain sensitive PII aside from requestors' names, and some requests are received through third party services (e.g., requestors' attorneys, or organizations that exist solely for the purposes of serving as third parties on behalf of FOIA requestors) and do not contain individuals' names. Records are sometimes retrieved by name in order to follow up on individual requests, although retrieval is most often by case number.

FOI Invoicing may contain contact information for FOI requesters as well as itemized accounts of charges invoiced for services and records of payments received. Retrieval from FOI may be by personal identifier (FOIA requesters' names). Retrieval from FOI Invoicing may be by personal identifier (FOIA requesters' names).

FOI OnLine Request Submission is a web-enabled tool. Requests do not reside on this application and are instead transferred to the FOI application. Retrieval from FOI Invoicing may be by personal identifier (FOIA requesters' names). FDA does not use PII to retrieve information from this application and it is not subject to the Privacy Act.

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

Financial Accounts Info

Any other unsolicited information the requestor chooses to include in a request letter

FOI and FOI Invoicing require application-specific credentials

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

Employees

Public Citizens

FOIA requests may be made by any person. While these requests may come from FDA employees, business partners, vendors, or anyone else, requests must be made in their personal capacity. FDA also accepts FOIA requests from non-citizens.

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

PII is used to respond to requests for information submitted under the Freedom of Information Act.

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

None.

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

Use and disclosure of information in FOI is governed by the Freedom of Information Act (FOIA), 5 U. S.C. 552. Responding to FOIA requests is a significant activity at many federal agencies, and the interpretation and application of its requirements often involve reliance on case law (i.e., court decisions) and other guidance. Neither NADA nor FOI Online Request Submission use or disclose PII (FOI Online Request collects PII but does not use or disclose it). While FOIA creates the need for and authority for the creation of these systems, neither requires a legal authority for using or disclosing PII because neither uses or discloses PII.

For the FOI Invoicing application, 5 U.S.C. 552 (a)(4)(A) establishes the conditions under which fees may be charged for responses to FOIA requests, and requires each agency to "promulgate regulations, pursuant to notice and receipt of public comment, specifying the schedule of fees applicable to the processing of requests under this section and establishing procedures and guidelines for determining when such fees should be waived or reduced."

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.

SORN 09-40-0012, Debt Management and Collection System (Applies to FOI Invoicing)

SORN 09-90-0024, User Fee Management System (Applies to FOI Invoicing)

SORN 09-90-0058, Freedom of Information Case Files and Correspondence Control Log (applies to

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Other

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

OMB approval may be necessary for this activity. The system point of contact will coordinate with the office responsible for requesting information collection approval numbers and initiate the approval process.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

Coordinate responses to FOIA inquiries, including locating and collecting relevant documents. FDA makes an effort to consistently share only the information necessary to identify and obtain the relevant documents.

Other Federal Agencies

Coordinate responses to FOIA inquiries, including locating and retrieving relevant documents. FDA makes an effort to consistently share only the information necessary to identify and collect the relevant documents. FDA may forward FOIA requests to other agencies' FOIA offices if they hold the information requested, and the appropriate other agency often chooses to then respond directly to the requester.

Describe any agreements in place that authorizes the information sharing or disclosure.

Analysts may contact other HHS Operating Divisions (OpDivs) or other federal agencies in the course of determining how to respond to FOI requests and where responsive records are held. Specific MOUs are not usually executed to conduct these exchanges which will differ case-by-case given the variety of requests.

Describe the procedures for accounting for disclosures.

Disclosures from these applications are unlikely to be made. If Privacy Act records are disclosed, the disclosing office will maintain an accounting. When necessary, the Privacy Office provides guidance to System Owners on what information must be maintained in an accounting of disclosures under the Privacy Act, 5 United States Code (U.S.C.) 552a(c).

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

Requestors submit all information themselves at the time of collection. For requesters that use the online FOIA request application, a Privacy Act Statement Notice is prominently displayed on the web page.

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.

Submission of FOIA requests is voluntary. However, the submission of PII is necessary in order to communicate and send responses to requests.

Submitters may not opt out of submitting PII if they wish to receive a response, because FDA would not know where to send the response nor who to contact to clarify requests.

Users of both of these applications are FDA employees, and the applications contain PII relevant to their access credentials. 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.

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

No such changes are anticipated. If the agency changes the collection, use, or sharing of PII data in these applications, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on the web site, or e-mail notice to the individuals.

If the agency ever used the PII of its employees that serve as access credentials, employees could be contacted many ways, including by phone, e-mail, notices on the intranet, and via changes to the SORN.

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.

Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system often use the FOIA process--or the related Privacy Act request process-- to make that determination. They then have a number of avenues available to request to rectify the situation. Often, these individuals contact the office or division where they have determined that their records are held. Requestors may then make further requests for their information to be corrected or amended. FDA considers these requests and, if appropriate, makes the requested changes.

Other avenues available include communicating directly with the FOIA office or assigned analyst to request corrections or additions.

Employees with such concerns can additionally work with their supervisors, a 24-hour technical assistance line, FDA's Computer Security Incident Response Team, and other channels.

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

PII is used transactional to address a specific business function (responding to FOIA requests). It would not represent a benefit to the public or to FDA to maintain PII and update or correct it after it has been used for the intended purpose. FDA employee users' access credentials are updated consistent with security practices.

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

Users:

Users are FDA employees requiring access to PII to perform their jobs. Users require full access to systems in order to conduct activities related to delegating and responding to FOIA analysis assignments.

Administrators:

Administrators grant access to FDA employee users based on each user's role and activities.

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 these applications 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 these applications on a quarterly basis to review and adjust users' access permissions, and to remove unnecessary accounts from these applications.

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.

All personnel/users are required to complete FDA's IT Security and Privacy Awareness training at least annually.

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

Most AdminApps applications have system documentation, including user manuals. FDA is currently reviewing system documentation to determine if this can be made freely available to all potential users via the FDA intranet, or if access to these can be made available but restricted through system access control.

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.

Information in the FOI and FOI Invoicing applications are retained under General Records Schedule (GRS) 14, Items 11 through 15. Files dealing with requests and initial responses must be retained for two years. Requests dealing with appeals must be retained longer (six years or more). Control files (registers and similar records listing date, nature, and purpose of request and name and address of requester) must be retained for five years after the last date of entry.

Information in FOI OnLine Request Submission requires a schedule and does not currently have one. A schedule is needed that addresses inputs from members of the public, i.e., FOIA requests submitted online and retained. Until a schedule is created and approved, records must be retained indefinitely.

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

Administrative Safeguards include training and awareness provided for all users; system manuals that advise on the proper use; implementation of Need to Know and minimum necessary principles when awarding access, and others. All FOI applications reside behind the FDA firewalls. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. More broadly, appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 500-53, as determined using Federal Information Processing Standard (FIPS) 199.

Identify the publicly-available URL:

http://www.accessdata.fda.gov/scripts/foi/FOIRequest/index.cfm

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

No

Does the website use web measurement and customization technology?

No

Sessions don't time out. Session cookie remains active as long as the user is accessing the web site.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null