US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/12/2016

OPDIV:

FDA

Name:

Administrative Applications: Communications Applications

PIA Unique Identifier:

P-4380566-680763

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?

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.

This PIA addresses two applications that reside within FDA's overarching AdminApps system: Correspondence, and Records and Case Management Systems.

Correspondence is an application that assists in the management, work flow, and tracking of responses to correspondence from external senders (such as Congress, media inquiries, and members of the public). Users of the Correspondence application can view header information for all items in the system (e.g., the name of the sender and the date the item was scanned into the application).

Records and Case Management Systems (RC) is a similar application, but was created to provide better privacy and security protections. Users of RC can restrict access to materials such that even the header information is visible only to those who are authorized to view these materials.

Note that neither system is accessed, used, or even viewable to the public. Correspondents send correspondence to FDA, and then FDA employees scan and enter these documents into these applications. Therefore, although the source of the contents of these applications is external to FDA, the system is entirely internal to FDA.

Aside from the security enhancements of RC, the systems are otherwise the same in terms of purpose and PII contained.

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

For both applications, information entered to record and track correspondence received includes the name of the sender of original communications (either an individual or an organization) and the date received; the actual document scanned includes any information the sender chooses to include, which may include PII, health information, proprietary information, or other sensitive information. Any type of information and any data elements may be contained in correspondence, and FDA does not solicit specific information, provide templates, or otherwise restrict the content of what information correspondents may choose to send to the FDA. Senders of communications could be any correspondent: A member of the public; a regulated institution or an individual representative thereof; a government official at the federal, state, or local level; a journalist; a student; an FDA employee (most likely, writing in his or her private capacity); or even a foreign citizen or institution. Records usually include draft and final copies of responses to correspondence including any attachments sent.

Users of the application are limited to FDA employees involved in logging and tracking correspondence; routing it to the correct recipients; responding to it; and ensuring it has been reviewed by all parties at the FDA whose input is necessary. Users may also be able to determine which offices or individuals have access to correspondence.

The Correspondence application was initially used only by FDA's Office of the Executive Secretariat and the Office of Legislation. Over time, other Centers (FDA component subagencies) were provided access in order to coordinate responses from these offices. Now, some Centers use these applications to manage their own correspondence, as well as coordinating responses at the agency-wide level.

Retrieval of records (from either system) may be by PII such as correspondent name. Categories of individuals (correspondents) whose name or other PII users employ to retrieve records may be any senders of correspondence to FDA including members of the public, employees, business partners, and any others. Users may also retrieve records using other information (non-PII) such as the date FDA receivedcorrespondence.

The Correspondence and RC applications require FDA users to have application-specific logon credentials (username and password).

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

Users (who are FDA employees only) upload scans of correspondence received from external correspondents and enter basic data concerning the sender, date received, and individuals authorized to view the materials. Other users are then able to view these materials, and to generate and upload responses. Users are able to track which individuals and offices have had an opportunity to review both incoming and draft outgoing correspondence. Currently, users are all FDA employees, although it is possible that FDA may choose to employ direct contractors who will need access to this system in the future.

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

Medical Notes

Financial Accounts Info

Certificates

Education Records

Military Status

Employment Status

Foreign Activities

These categories of information are those that FDA believes to be the most common categories of

The Correspondence and RC applications require FDA users to have application-specific logon credentials (username and password).

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

PII is usually limited to information identifying the sender of correspondence and is used to address responses to that individual. Less often, PII may be provided that is relevant to an inquiry, complaint, or concern, such as information concerning an adverse health event, provided by the sender to request assistance or action on the part of an FDA Center (i.e., one of the eight component organizations of the FDA) or authority.

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.

Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321 et seq.); the Public Health Service Act (42 U. S.C. 201 et seq.), and authority delegated to the Commissioner (21 CFR 5.1).

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.

09-10-0004, Communications (Oral and Written) With the Public, HHS/FDA/OC. SORN applies to

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Other Federal Entities

Identify the OMB information collection approval number and expiration date

Not Applicable.

Is the PII shared with other organizations?

Yes

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

Within HHS

PII is shared within HHS as necessary to respond to a public inquiry. For example, if a correspondent requests information most of which is held by FDA but some of which is held by another HHS Operating Division; and if providing the name of the requestor will help FDA explain to the other OpDiv what information is being sought, it is possible FDA will disclose the requestor's PII in order to fulfill their request.

Other Federal Agencies

Information may be shared with other Federal entities if sharing PII is necessary to respond to a public inquiry. For example, if a correspondent requests information most of which is held by FDA but some of which is held by another federal agency, and if providing the name of the requestor will help FDA explain to the other agency what information is being sought, it is possible FDA will disclose the requestor's PII in order to fulfill their request.

State or Local Agencies

FDA may share PII with state and local entities if necessary to respond to a public inquiry. For example, if a correspondent requests information most of which is held by FDA but some of which is held by a state or local agency, and if providing the name of the requestor will help FDA explain to the other agency what information is being sought, it is possible FDA will disclose the requestor's PII in order to fulfill their request.

Private Sector

FDA may share PII with private sector entities if necessary to respond to a public inquiry. For example, if a correspondent requests information most of which is held by FDA but some of which is held by an FDA-regulated business, and if providing the name of the requestor will help FDA explain to the regulated business what information is being sought, it is possible FDA will disclose the requestor's PII in order to fulfill their request.

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

FDA may need to make certain disclosures in order to respond to requests. For example, it is not uncommon for FDA to receive Congressional inquiries made on behalf of constituents. FDA may share information it holds, and may coordinate with other organizations, to provide a complete response. In the course of generating that response, it would be appropriate for FDA to note the name of the Congressperson requesting the information and the Congressperson’s business contact information, and to supply PII of the constituent back to the Congressperson. The FDA does not anticipate that these conditions come up often, but will execute usual and appropriate business practices to address these with appropriate confidentiality.

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 disclosure 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.

PII about individual correspondents is submitted by the individuals themselves via communications made to the FDA. This information is not solicited, requested, or restricted by the FDA, and advanced notice is therefore not possible for FDA to provide. Correspondents, however, will of course be completely aware of what information they have voluntarily and of their own initiative sent to the FDA.

System user account access credentials are provided to the users in the course of their employment.

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.

Correspondents provide any and all PII voluntarily. Correspondents will need to provide contact information if they wish to receive return correspondence.

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.

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). For correspondents, this may include a notice on the FDA web site, or an e-mail notice to the individuals (if e-mail addresses are provided). FDA employees would be notified through any number of channels including e-mail, phone, updates to the applications, through supervisors, andor by updates in 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 are the subject of records in these applications (i.e., correspondents) may exercise the rights available to them under the Privacy Act. The Privacy Act permits information subjects whose records are retained in systems of records to request notification of the existence of, access to, and amendment of records about themselves.

Individuals may also address these concerns by contacting the party to whom they originally sent correspondence. The recipient FDA staff members have many avenues through which to provide assistance, including through an FDA help desk or its Computer Security Incident Response Team.

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 HHS's human resources information system.

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

Information in this application is transactional. Individuals sending correspondence are responsible for providing complete, accurate, relevant information.

FDA personnel are responsible for providing accurate information and may independently update and correct their information at any time.

For all PII, availability is protected by security controls selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined to be appropriate based on risk level 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:

Individuals who contribute to responses to correspondence or provide reviews will have access to PII in order to perform these functions.

Administrators:

Administrators conduct management and oversight of the application, including managing access for system users requiring new or modified access.

Developers:

Developers will not normally have access to PII, but may in the course of maintaining the applications 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.

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).

Help links are available from within the applications, and additional instructional materials are available on the FDA intranet. Access to training 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 application. 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.

Correspondence is maintained under FDA File Code 8111 for Significant Correspondence, NARA code N1-088-06-3). Retention for this correspondence is permanent and the records are never destroyed. Non-Significant Correspondence is maintained under 8112 (NARA N1-088-06-3) maintained for at least ten years, and is then disposed of unless the record is still in active use.

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; application manuals that advise on proper use of the applications; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include that PII resides 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 800-53, as determined using Federal Information Processing Standard (FIPS) 199.