US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/04/2016

OPDIV:

FDA

Name:

Recall Enterprise System

PIA Unique Identifier:

P-9180297-810413

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The system has been enhanced to provide Recall Coordinators with the ability to create and/or update assignment requests for Recall Audit Check (RAC) field work; to create, upload, and manage distribution lists; to generate RAC summary reports; and to view RAC status and completed FDA forms 3177 (RAC Report).

Describe the purpose of the system.

The Food and Drug Administration's (FDA) Office of Regulatory Affairs (ORA) Mission Accomplishment and Regulatory Compliance Tracking - Recall Enterprise system (RES or MARCS Recalls) is an internal system that automates the process by which FDA-regulated products are removed from the marketplace. RES automates FDA's identification, processing and tracking of health and safety alerts and product recalls. RES provides centralized safety and health alert information, and, regulated product recall information. FDA alerts and recalls are an effective method of providing alert notices to the public and firms, and for removing or correcting consumer products that are in violation of the laws administered by the FDA.

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

Information collected, maintained or shared in support of FDA's recall of regulated products focuses on the Recall Event, Recalled product's Firm and Recalled product.

For Firms associated with the product being recalled, information includes: Responsible Firm Name, Manufacturer Firm Name, Firm Address as well as business contact information (Title, Name, Address, Phone, Fax, Email) for the Firm's "Most Responsible Individual." This individual is the person with whom the FDA will communicate when notifying the Firm that its action meets the definition of a recall and that FDA has assessed the hazard level of the relevant product(s). This individual's name, title, and work address are often publicly available, particularly if the Firm is traded on the stock market. In rare circumstances, particularly with small firms, the business address may be the same as the individual's home address. Additionally, RES captures information about the Firm's "Recall Contact." This is the individual at the Firm that is providing recall information to the FDA. In support of FDA Form 3177 (FDA Recall Audit Check Report, completed by FDA personnel), RES captures the name of the Recall consignee (custodian/transporter of a product subject to recall) as well as the potential explanation from the consignee regarding their awareness of any injuries, illness or complaints associated with a recall.

For a Recalled product, information includes: Product Name, Description, Trade Name, Model, Lot, Volume, Usage, and Shelf Life.

For the FDA Recall Event, FDA recall-specific information includes: Event ID, Recalling FDA Center, District, Date, Reason, Status, Public Reason for Recall, Evaluation, FDA Recall Coordinator Contact, Root Cause, FDA Center Comments, Type of Injury, Complaints, Recall Strategy, Consignees, Preventative Action, District Follow-up & Review, Legal Action.

RES also holds names and e-mail addresses of Recall Coordinators and other FDA employees who create or work with system records. This information is necessary to manage data collection needs related to the recall event, for work flow processing, and for the application to submit proper notifications. This information is supplied by the FDA's Field Accomplishments and Compliance Tracking system (FACTS) database, and includes information regarding each user's role, and the FDA Center with responsibility for oversight of a recall activity.

Comment fields are available within the RES system in which the RES users will add necessary information, when applicable, in order to ensure information is provided for "recall" requirements.

The system is accessed by single sign-on and no usernames or passwords are stored in the system. Users are all FDA employees and direct contractors.

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

This system automates FDA's identification, processing and tracking of health and safety alerts and product recalls. In order to effectively do so, the system collects information about products and certain contact information for individuals.

As detailed elsewhere in this assessment, RES contains work contact information for a Firm's "Most Responsible Individual," with whom FDA will communicate when notifying the firm of a recall and FDA's assessment of the hazard level of the relevant product(s). This individual's work contact information is often publicly available. In rare circumstances, particularly with small firms, the business address may be the same as the individual's home address.

The system also contains the name, title and work contact information for a firm's “Recall Contact,” the individual at the firm that is providing recall information to the FDA. Likewise, RES captures the name of any recall consignee (custodian/transporter of a product subject to recall) and the consignee explanation regarding their awareness of any injuries, illness or complaints relevant to a recall.

The system also holds names and e-mail addresses of FDA personnel such as Recall Coordinators who create or work with system records. This information is necessary to manage data collection, for work flow processing, and for internal notifications. This data is supplied by a separate FDA system, the FDA’s Field Accomplishments and Compliance Tracking system (FACTS) database, and includes information regarding each user’s role, and the office overseeing a recall activity.

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

PII collected is work contact information for industry points of contact, and in fewer cases for FDA

PII collected is work contact information such as mailing address, e-mail, phone and work e-mail.

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

Employees

Public Citizens

Note, "Public citizen" refers to the external points of contact involved in a recall. "Employees" includes Direct Contractors performing work for HHS/FDA.

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The PII, consisting of business contact information for FDA personnel and industry points of contacts, is collected for communicating with firms in relation to recall activities, and tracking and managing FDA's processing and administration of the activity.

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.

FDA uses this system to protect and promote the health and safety of the American public under the Federal Food, Drug and Cosmetic Act (21 U.S.C. 301) and the Federal Records Act.

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

No

Not Applicable.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

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.

At the time of hire, FDA/HHS notify agency personnel and as a condition of their employment obtain consent to FDA's use of their information in relation to their work with FDA. Industry contacts submit their work contact information in the context of recall activities and are aware of FDA's use of their information. Individuals may also view FDA's website and privacy policies permanently available via link on all FDA intranet and internet pages.

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.

While submission of PII is "voluntary" as that term is used in the Privacy Act, there is no option to opt-out. The PII is required in order to communicate with the firm points of contact in regard to product recall activities. The selection of the firm point of contact (POC) is at the discretion of the regulated industry, provided that person is the "Most Responsible Person" as indicated in the filing requirements.

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

If there are major system changes impacting use of PII, FDA will assess the need to notify individuals and implement appropriate notice mechanisms such as e-mail or letters to firm contacts and/or posting notices online.

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.

Personnel may contact IT security to report a potential privacy incident, may contact the FDA Privacy Office, and may seek assistance through FDA's Employee Resource and Information Center (ERIC). Firm points of contact may submit concerns to their FDA liaison or other agency offices using the mailing addresses, email addresses and phone numbers available on FDA.gov.

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 accuracy and relevancy is promoted by providing individuals and organizations with the ability to update and correct their information. FDA personnel are directed to keep their office information current and can update or correct their information at anytime. Firms and their points of contact are responsible for submitting accurate current contact information, and updating this information as needed by contacting FDA. Incorrect or out-of-date information is also addressed when identified in the course of system use.

Information integrity and availability is protected by Administrative and Technical security controls.

Administrative controls to protect availability include user training, and implementation of need to know and minimum necessary principles when awarding access. Technical controls to protect integrity include uses of access controls such as single sign-on with multi-factor authentication; and regular testing of information technology systems.

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

Users:

Process and Manage Data Submission of recalls.

Administrators:

Review, process and administer the system, files and data as well as access control.

Developers:

Troubleshoot issues with the system, performance and access.

Contractors:

Support the IT team for administration, troubleshoot and development of the system.

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

Users who require access to the information system must first obtain management approval before being granted access to RES. This approval is requested and documented via an access request and account creation form that is required by standard procedure. Users granted access to RES must have a need for access in order to perform their job function. Approving management confirms the individual's role and need for access.

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.

Supervisors indicate on the account creation form the minimum information system access that is required in order for the user to complete his/her job. The access list for the information system is reviewed on a quarterly basis and users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system.

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 users are trained on the system, and all users must annually complete FDA's information security and privacy awareness training.

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

Users receive system-specific training, and may obtain additional privacy guidance from the agency's privacy officials.

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.

Recall action records fall under FDA File Code families 7100 (7110) and 8100 (8120), and NARA approved citation N-1-088-05-01. Record destruction schedules vary by subtype and range from four to 75 years after close of a recall action.

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

FDA employs numerous technical, physical and administrative safeguards to protect PII and other data in the system. Safeguards include supervisor access controls, user identification, passwords, firewall, encryption, virtual private network, intrusion detection, guarded facilities and closed circuit TV.