US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/17/2016

OPDIV:

FDA

Name:

Compliance Management System

PIA Unique Identifier:

P-1025627-042526

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?

No

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)?

No

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.

PIA Refresh

Describe the purpose of the system.

The Mission Accomplishment and Regulatory Compliance Services Compliance Management System (MARCS CMS) is the FDA enterprise-wide compliance system. CMS provides mission critical functionality allowing the assembly and integration of information from various FDA systems such as the Field Accomplishments and Compliance Tracking System (FACTS), Operational Administrative System for Import Support (OASIS), Private Lab Analysis Tracking System (PLATS), Facility Management System (FMS), Enterprise Administrative Support Environment (EASE) and FDA Unified Registration & Listing System (FURLS) which all are assessed under separate Privacy Impact Assessments (PIAs). Within the CMS system, the data from these systems are organized around the firm (e.g., FDA regulated entity) and Facilities Establishment Identifier (FEI) to support the workflow of evaluating potential compliance enforcement actions involving a regulated entity.

This system is the cornerstone of FDA's enforcement activities. It supports uploading documentation and evidence, and the flow of the information to all pertinent parties within FDA. MARCS CMS provides tools supporting FDA field employees and FDA compliance officers who process compliance actions and work activities. All personnel who access CMS are FDA employees and direct contractors, including District Office Freedom of Information Act staff. Unless otherwise indicated in this assessment, the sources of PII in this system are contained within other FDA systems and notice, consent and other privacy protections are provided by those systems. Personnel do not retrieve information in this system by name or other personal identifier, but by case file number or name of a regulated institution.

MARCS CMS core functions include:

Electronically tracking compliance information and supporting the recording of all decisions for easy reporting on FDA compliance.

Reporting, analyzing, and evaluating compliance data to assess FDA's enforcement activities; allowing users to review whether a compliance action should be taken against a firm.

Enhancing and streamlining the Warning Letter process.

Processing and publicizing Import Alerts (IA) and Bulletins.

Forwarding warning letters to the Division of Freedom of Information for publication to the web. The Freedom of Information office reviews, redacts (when necessary) and manually enters letter information into a separate web publishing tool used to post the public information on the web (fda.gov). FDA proactively publishes this information on the web for purposes of transparency, public awareness of FDA actions and because it is frequently requested under the Freedom of Information Act. The CMS application itself does not publish to fda.gov and is not interconnected to the web publishing tool.

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

MARCS CMS contains inspection and investigative records, sample collection reports, analytical worksheets, open investigatory files and other records supporting FDA's administrative and legal actions, including issuance of warning letters and untitled letters as compliance actions. FDA uses records in CMS to track and accurately associate clinical research investigators with a regulated activity, monitor complaints submitted to FDA, and support FDA inspections and related administrative or legal actions. The evidence gathered during inspections and sample collections can be used against a firm if the FDA takes action.

MARCS CMS files may also contain personally identifiable information (PII) in the form of individual consumer names when referenced in consumer complaints or in medical records obtained during FDA inspections, investigations or other legal and administrative actions. This information is maintained in and drawn into CMS from other FDA applications such as FACTS, OASIS, FMS, EASE and FURLS.

CMS records also contain PII in the form of names of clinical research investigators. Clinical investigators are typically employed by regulated research and clinical trial sponsor entities but may also be self-employed. They are responsible for overseeing a research trial or study. In some instances the business entity or firm name is the clinical research investigator's name, such as a sole proprietorship operated by the clinical research investigator. Clinical research investigator names and identifiers such as mailing address or work e-mail addresses are typically provided voluntarily or on occasion by demand of FDA. Consumer names are voluntarily provided directly to FDA or gathered as part of FDA inspections or investigations.

Because this system contains individual names and personal identifiers, access to it is strictly controlled. FDA employees enter this information online through the CMS system.

Individuals with access to CMS are all FDA employees and direct contractors. Access to CMS is through the multi-factor authentication process also known as single-sign on. Individuals accessing CMS do not authenticate to the system using a system-specific username and password.

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

MARCS CMS is a web-based application accessed and used solely by FDA employees and direct contractors. It is not for the use of the general public nor any other external individual or entity. CMS provides FDA's District (field) and Center Compliance Officers the ability to create, assign and track the review and completion of Compliance Actions and Work Activities. The MARCS CMS application also provides users with the ability to run and save reports related to the Compliance Action and Work Activity data, including but not limited to, inspections, sample collections, firms, and import alerts.

Information in CMS is gathered from FACTS, OASIS, FMS and FURLS and displayed on the screen for FDA reviewers to view. Notification to a regulated organization would be via a warning letter, import alert or similar memo that is stored in CMS. FDA reviews and redacts warning letters, then posts them on FDA.gov. CMS stores the redacted warning letters internally, but FDA does not use CMS use to post warning letters to the web.

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 Records Number

Medical Notes

Legal Documents

Work e-mail addresses are for FDA employees and direct contractors accessing the CMS system. Clinical research investigators submit their names, phone numbers and mailing addresses and have the option of submitting their work e-mail address as well. The specified data items are the most frequently collected types of PII. The data is information contained in documents that are relevant to an evaluation of compliance. Legal documents refers to warning letters.

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

Employees

Public Citizens

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

"Employees" refers to FDA personnel and direct contractors who use the system. "Public Citizens" refers to individual employees of regulated entities including clinical research investigators, and consumers whose names are voluntarily provided to FDA or gathered as part of FDA inspections or investigations.

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

PII is used to manage workload, plan actions and assignments (e.g., inspections), track activities and contact relevant individuals. These records are used to track clinical research investigators, to monitor complaints submitted to FDA, and in support of FDA inspections and related administrative or legal actions.

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 MARCS CMS 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); the Federal Records Act; Information Technology Management Reform Act (also known as the Clinger-Cohen Act of 1996); the E-Government Act of 2002, Title III, Federal Information Security Modernization Act of 2014; and Executive Order 13231.

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

No

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

Yes

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

Within HHS

Within FDA only. If the FDA determines criminal enforcement is necessary, the relevant information would be sent to investigative/enforcement offices within HHS only.

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

N/A

Describe the procedures for accounting for disclosures.

N/A

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 personnel are given notice of and consent to FDA's use of their professional information in relation to their work as a federal/FDA employee. Consumer names are voluntarily provided directly to FDA or gathered as part of FDA inspections or investigations. Clinical research investigator names and identifiers are typically provided voluntarily or on occasion by demand of FDA.

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.

FDA personnel are required to provide their name and work contact information in order for the system to function. External individuals provide PII voluntarily or when required in the context of a regulatory action.

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

If FDA practices change with regard to the collection or use of PII in CMS, the agency (or HHS human resources offices in the case of agency personnel) will employ appropriate notice and consent procedures such as e-mail to individuals, and adding or updating forms or online notices and disclaimers.

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 raise concerns and/or submit data corrections through supervisory channels and FDA's Employee Resource and Information Center (ERIC). Individuals who are not FDA employees or contractors may contact FDA through numerous e-mail, phone and standard mail avenues (all listed 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.

PII for FDA personnel is obtained via FDA's EASE system. The HHS Enterprises Human Resources Payroll Program (EHRP) system is the source of data in EASE. FDA personnel and direct contractors may correct/update their information.

Consumer and entity point of contact PII is submitted by the individual and its accuracy is subject to the submitter. Data discrepancies identified in the course of system use are addressed when discovered.

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

Users:

Create, track and report on regulatory activities related to compliance management.

Administrators:

Create, track and report on regulatory activities related to compliance management.

Contractors:

Direct contractors conduct Help Desk research to assist users.

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

System access requests are reviewed and approved by the system/business owner along with the CMS management team. System accounts are reviewed on a regularly basis to determine if access is still required for each user. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based 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 when accounts are created to apply 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 FDA personnel complete mandatory security and privacy awareness training at a minimum of once a year.

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

Users are trained by the FDA Office of Enforcement and Division of Human Resource Development (DHRD).

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.

MARCS CMS falls under the approved National Archives and Records Administration citation number N1-088-09-003 which calls for deletion of records after specific time periods based on the nature of the record, e.g., administrative records in the system to be deleted 10 years data becomes obsolete or when no longer needed for administrative, operations or reference purposes, whichever is later.

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 multi-factor authentication, use of secure sockets layer (SSL) and others. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, require Personal Identity Verification (PIV) cards 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.