US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/16/2016

OPDIV:

FDA

Name:

Enterprise Document Management Platform

PIA Unique Identifier:

P-2984044-254332

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)?

No

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

PIA Validation

Other...

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

Upgraded from Documentum 5.3 to version 6.7. Documentum is FDA’s Electronic Document and Records Management Platform.

Describe the purpose of the system.

FDA's Enterprise Document Management Platform (EDMP) is a back-end system that provides an internal shared content and records management platform for the FDA and its Centers. The agency’ s various Centers have different business rules governing their use of the EDMP, but all employ it to store, retrieve and distribute electronic records internally through Center-specific interfaces. FDA Centers and components which employ the EDMP include the Center for Drug Evaluation and Research (CDER), Center for Devices and Radiological Health (CDRH), Center for Food Safety and Applied Nutrition (CFSAN), Center for Tobacco Products (CTP), Center for Veterinary Medicine (CVM), the Office of the Commissioner (OC), and the Office of Regulatory Affairs (ORA).

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

EDMP is a document and records management system. From a system perspective all documents show up as a documents. There are not specific data fields that relate to PII data. Standard document data fields include document name, document title, document subject, and document keywords. The system allows end users to enter into these fields what their organization determines is important in relation to the document.

The EDMP system is used by FDA personnel as a back-end tool for internal records management and internal content sharing. Members of the public do not have access to the system or data therein, and they are not permitted to submit PII or information directly to EDMP.

EDMP is a robust, flexible platform that supports enterprise (agency-wide) content management applications. The system provides a set of products and services that work together, in varying combinations, to meet the content and records management needs of FDA organizations.

This system is not designed or dedicated for use as a PII or sensitive information collection tool and the EDMP does not explicitly collect PII. EDMP will naturally contain a wide variety of information related to the different needs of offices and personnel across the agency. In order to effectively serve its purpose as a platform enabling personnel to manage an indeterminate variety of work-related materials, EDMP does not technically prevent users (authorized FDA personnel and Direct Contractors) within the agency from storing documents that may or may not contain PII or any other particular type of information.

The EDMP system utilizes single sign-on access with multi-factor authentication. There are no logon credentials stored locally within the system.

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

The data maintained in the system varies by user and program. EDMP is used for the internal management and sharing of substantive work materials without regard to specific content.

This system is not intended to function specifically as a tool enabling FDA to collect and maintain PII. The EDMP system does not explicitly collect PII. The storing of any content containing PII is voluntary and at the discretion of the user. Users are neither required to store nor prohibited from storing work-related materials, with or without PII, in EDMP.

Given the variety of data type/sensitivity users may store in EDMP, FDA applies a high level of security to EDMP. The EDMP system utilizes single sign-on access with multi-factor authentication. There are no logon credentials stored locally within the system.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

EDMP does not explicitly collect any PII. Users are neither required nor prohibited from storing work-related materials, with or without PII.

Whether, and what, PII may be contained in materials users choose to maintain in the system is a matter of individual users' discretion.

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

Due to the variety of user needs and potential stored data types, the system may hold PII for all or none of these categories of individuals.

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

Because EDMP is a document storing system used FDA wide the content of EDMP is potentially unlimited and the purpose of use of PII (if any) stored in the system will likewise vary. It is the responsibility of the party that has generated and contributed the document to EDMP to adhere to any use and disclosure restrictions, ensure authority to collect, satisfy access rights, and follow other applicable laws and policies.

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. 301, including sections 353, 355, 356b, 360 and 379k; Public Health Service Act, 42 U.S.C. 201, including sections 262, 263a.

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

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.

EDMP is not designed or intended to collect PII. Any PII within materials that users store in EDMP is initially collected by other systems which will be covered by their own PIAs. Organizations maintaining the point of collection system would be responsible for providing any required notice and choice to individuals.

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.

Individuals cannot opt out of the collection of their information because the system is not designed to collect or disseminate PII. It will simply store information as uploaded by internal FDA users. Opt-out methods would be presented to individuals by the organization conducting the initial collection of PII, which is not this system.

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

If there is a major change in FDA's privacy practices or its collection, use, or sharing of PII data in the EDMP, FDA will provide any required notice to the individuals in the most efficient and effective form available and appropriate to the specific change(s). This may include establishing a formal process involving written and/or electronic notice through the source system. Alternatively, notification will be made by informal processes such as e-mail notice to the individuals affected. The system is not designed to collect or disseminate PII. It will simply store information as uploaded by internal FDA users.

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.

Because EDMP is an internal back-end system not specifically designed or intended to collect PII there is not a dedicated notice or complaint process within EDMP. Organizations maintaining other systems that are the point of PII collection would be responsible for providing any required notice and/or complaint process.

Employees have the options of reporting loss, misuse, or inaccuracy of PII to supervisors; to the Computer Security Incident Response Team; to a 24-hour Help Desk; or to the office they believe has been involved with a misuse or inaccuracy.

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

Not Applicable. Organizations maintaining other systems that are the point of PII collection would conduct any PII validation and availability actions.

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

Users:

Authorized users may view content subject to the rules applied by each secure area’s Center.

Administrators:

Individual administrators may have access to PII within the content to which they have authorized need to know access; they are not able to view non-explicitly authorized content and are subject to FDA rules and regulations on use and access.

Developers:

Developers are not able to view non-explicitly authorized content and are subject to FDA rules and regulations.

Contractors:

Users may only view authorized content, which may contain PII, and are subject to FDA rules and regulations.

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

Each secured area in EDMP is explicitly managed by one or more secured/controlled area owners designated by the owning Center. These owners must explicitly authorize access to any secured area. A secured area may or may not contain documents that contain PII.

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.

EDMP access permissions, assigned by Centers, are employed to determine who within FDA can access specific areas within EDMP and any uploaded documents therein that may or may not contain PII. Each secured area in EDMP is explicitly managed by one or more secured area owners designated by the owning Center. These owners must explicitly authorize access to any secured area. A secured area may or may not contain documents that contain PII.

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 must complete FDA's annual security and privacy awareness training. Training and awareness information may also be provided by the Center that authorizes access to the given secured area in EDMP.

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

EDMP systems administrators assist secured area owners to implement access permissions. The EDMP support team is instructed not to view the contents of any secured area that they are not explicitly authorized and required to view as part of their support responsibilities.

Privacy guidance resources are available to personnel on a central agency intranet page. Personnel may also take advantage of privacy awareness and role-based training offered by the agency's privacy experts.

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.

Users who store records within EDMP are required to retain them in accordance with applicable FDA Records Control Schedule and NARA General Records Schedule retention requirements. The records, and relevant control schedules, vary based on the nature of the repository and work of each related user/Center.

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

The information in EDMP is secured within data hosting centers and protected by administrative, physical, and technical controls in accordance with policies and regulations from the FDA, NIST, and OMB. Security controls are reviewed on a periodic basis to ensure that they are implemented correctly, operating as intended, and producing the desired result of protecting all information within the system. In view of the variety of data type/sensitivity users may potentially store in EDMP, FDA applies a high level of security safeguards to EDMP. Access requires the use of the personal identity verification (PIV) card and the system does not contain usernames and passwords.