US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/10/2017

OPDIV:

OS

Name:

Federal Records Enterprise Electronic Document

PIA Unique Identifier:

P-1091455-001462

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Test

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.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Describe the purpose of the system.

The Federal Records Enterprise Electronic Document Management System (FREEDOM) is an Electronic Records Management (ERM) system to manage both active documents and official records in the federal government domain. The solution is offered in a Software as a Service (SaaS) platform to provide federal agencies the means to implement a fully National Archive Records Administration (NARA) compliant ERM system.

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

FREEDOM serves as a repository for standard file types and content such as Microsoft Word, Excel, Powerpoint, and Portable Document Format (PDF) files.

Information that is stored within FREEDOM includes:

Intrafund Agreements, Customer Service Agreements, and Inter Agency Agreements which may include: Names, phone numbers, and email addresses of agreement stakeholders.

Financial Information including Dollar Amount Obligated, Common Accounting Number (CAN) and US Treasury Account Symbols (TAS)

Human Resources Personnel information which may include names, mailing addresses and social security numbers.

Food and Drug Administration (FDA) Federal Shelf Life Extension Program (SLEP) Testing and Analysis Documentation

Access is granted to FREEDOM by the use of internal Sharepoint permissions and groups. These permissions are managed by System Administrators and Agency Support Non-Direct Contractors where credentials are stored on the system.

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

FREEDOM's infrastructure is based off of Microsoft SharePoint platform, but with a customized easy to use interface. It is offered as a Software as a Service (SaaS) and is not external facing.

FREEDOM is an Electronic Records Management System that currently collects and stores:

Intrafund Agreements, Customer Service Agreements, and Inter Agency Agreements which may include: Names, phone numbers, and email addresses of agreement stakeholders.

Financial Information including Dollar Amount Obligated, Common Accounting Number (CAN) and US Treasury Account Symbols (TAS)

Human Resources Personnel information which may include names, mailing addresses, and social security numbers.

Food and Drug Administration (FDA) Federal Shelf Life Extension Program (SLEP) Testing and Analysis Documentation

Access is granted to FREEDOM by the use of internal Sharepoint permissions and groups. These permissions are managed by System Administrators and Agency Support Non-Direct Contractors where credentials are stored on the system.

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

Yes

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

Social Security Number

Name

E-Mail Address

Mailing Address

Phone Numbers

Financial Accounts Info

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

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

To serve as a repository to collect, store, and search for key documents. It is only accessible to interrnal users of the system.

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

None

Describe the function of the SSN.

The SSN is used in support of the HHS Program Support Center Office of Human Resource Operations. The SSN has been encrypted in transit and at rest and is limited to a few key internal end users with elevated privileges and behind the HHS firewall.

Cite the legal authority to use the SSN.

The Public Health Service Act (42 United States Code (U.S.C.) 202-217, 218a, 224, 228, 233, and other pertinent sections); The Social Security Act (42 U.S.C. 410(m) et seq.);

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

The development and implementation of this system are conducted pursuant to 5 U.S.C. Sec. 301

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Government Sources

Within OpDiv

Other HHS OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Not applicable. The information in FREEDOM is not collected directly from the public.

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.

FREEDOM's source of Personally Identifiable Information (PII) originates from paper documents. They have been previously collected and consolidated by the individual's themselves, their respective Operating Division, or Human Resources Department as either a condition of employment or to perform the function and duties of their organization. As a result, there is no opt-out method in place.

For internal users, the login banner states the conditions that must be agreed upon in order to access the system. It states that internal user's actions are monitored while accessing FREEDOM.

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.

They have been previously collected and consolidated by the individual's themselves, their respective Operating Division, or Human Resources Department as either a condition of employment or to perform the function and duties of their organization. As a result, there is no opt-out method in place.

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

There is no process in place to notify individuals whose PII is in FREEDOM. FREEDOM's source PII originates from paper documents that have been later scanned. The Federal Agency's source of the paper documents is responsible for the process to notify and obtain consent from the individuals whose PII is in the system.

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.

The individual can contact the System Owner or Administrator for the specific Sharepoint module. They also have the right to file a Health Information Privacy Complaint with the HHS Office of Civil Rights.

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

There are no processes in place for periodic reviews of PII contained in the system for personnel files. These files are for historic (some dating over 50 years back) and have been archived for search purposes.

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

Users:

Required to manage documents which may contain PII based on access level.

Administrators:

Required to manage documents which may contain PII depending on the access level.

Developers:

Maintain the system which contains PII.

Contractors:

Required to scan hard copies of files containing PII to be transferred into Sharepoint. They are non-direct contractors

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

System end users permissions are defined by the administrator at the time the account is created. Permissions include access to specific work flows, read/write and what libraries they can view.

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.

Appropriate access is granted to the system based on predefined roles and job descriptions. System owners are responsible for creating the proper security groups within their system with applicable permissions for group members to enforce least privileges.

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 all Privacy and Security Training before access is granted. In addition, privacy and security is required on an annual basis as a refresher in order to maintain access.

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

All end users receive training upon initial access to the system. In addition, there are help files, training videos, and on-site or web-ex training whenever needed.

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.

When a document becomes an official record, it is required to select the corresponding record schedule based on NARA's Electronic Records Archives (eRA) system. FREEDOM's ERM workflow will automatically trigger a notification when a record's retention schedule is met in order to destroy or automatically transfer to NARA eRA.

The records in FREEDOM will be retained and disposed of in accordance with the National Archives and Records Administration’s (NARA) General Records Schedule (GRS) 2.2 Employee Management Records, GRS 3.1 General Technology Management Records, GRS 3.2 Information System Security Records, GRS 4.1 Records Management Records

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

FREEDOM is behind the HHS firewall. Access to FREEDOM requires an HHS Government furnished laptop, Personal Identity Verification (PIV) Card, and a least privileged account to the FREEDOM system. FREEDOM also follows the National Institute of Standards and Technology (NIST) 800-53 Risk Management framework in order to obtain an Authorization to operate. PII information is encrypted both in transit via Secure Socket Layer (SSL) and at rest. If FREEDOM is unable to meet a security requirement, HHS will issue a Plan of Action and Milestone (POA&M). At this point, the FREEDOM Information System Security Officer (ISSO) will work with system engineers to ensure the security weakness is remediated as soon as possible.