US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/24/2017

OPDIV:

CMS

Name:

CMS SharePoint

PIA Unique Identifier:

P-4454236-655105

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.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

CMS Agency SharePoint (CMS Share) and CMS Agency Project Management System (CAPMS) is a Microsoft application, web based collaboration and project management tool. It is used to facilitate the sharing and storing of documents, sharing calendars, creating document workflows, announcements, and helpful links. The documents stored in CMS Share and CAPMS may consist of standard operating procedures, policy documents, and helpful notes and frequently asked questions to support CMS components in effectuating their business.

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

CMS Share/CAPMS serves as a repository for standard file types and content such as MicroSoft Word, Excel, Powerpoint, and Portable Document Format (PDF) files.

Business components and units within CMS may use sensitive information including PII and PHI to form groups of records. For example, SharePoint will store technical and business architecture documents, CMS budget requests and funding reports, medicare claims records, beneficiary records, contract and vendor proposals, proprietary vendor and product information, human resource documents such as resumes and job proposal letters, employee salary and promotion documents. The documents will be used to support internal CMS business processes. Potentially, other Information may be uploaded to SharePoint such as Social Security Number, Name, E-Mail Address, Phone Numbers, Medical Notes, Education Records, Date of Birth, Mailing, Address, Medical Records Number, Financial Account Information, Legal Documents, and Employment Status.

CMS Share is the CMS configured version of SharePoint and acts as a collaborative cross-agency platform where each business component has its own site and data/content specific to its business processes.

CAPMS is a project management focused application that resides on CMS SharePoint. The content used by CAPMS is primarily CMS project management data, such as project schedules, milestones, tasks, dates, etc.

Access is granted to SharePoint collaboration sites by use of internal Sharepoint permissions and groups. These groups are managed by business component Microsoft Access Managers, Site Administrators, and the agency SharePoint support contractor (CMS direct contractors)- TTC, Inc.

This system may contain sensitive information including unsolicited PII and PHI based on the needs of the CMS organizational customers.

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

SharePoint is a Commercial Off the Shelf (COTS) web-based Microsoft application. CMS Share is the CMS configured version of SharePoint and operates on the CMSNet/intranet and is not externally facing. CAPMS is a project management application that resides in SharePoint, and collects and stores project management data that may include names, medical record number, SSN, education records, email, and phone numbers.

CMS Share/CAPMS provide a business solution that facilitates sharing and collaboration of data within the agency. Specifically, SharePoint provides a tool for: Creating a shared collaboration space for documents, calendars, announcements, contact lists, and other important business information; automating and standardizing repeatable business processes; consolidating disparate information and tools into a single, easy to use interface; making important information and documents easily accessible to offices, groups, divisions, and project teams; and reducing or removing the need to e-mail large file attachments.

PII is may be collected from existing core applications. SP is not the primary system for data collection.

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

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Legal Documents

Education Records

Employment Status

This system may contain sensitive information including unsolicited PII and PHI based on the needs

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

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

PII is used to manage and index lists, libraries, and content for quick access and retrieval by business owners and system users. PII will also be used for data analysis and reporting.

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

There are no secondary uses of PII.

Describe the function of the SSN.

This system does not require the use or collection of SSN, however, the users of SharePoint/CAPMS may potentially upload the SSN.

Cite the legal authority to use the SSN.

The legal authority is Departmental Regulation 5 USC 301.

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

The legal authority is Departmental Regulation 5 USC 301.

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

No

Identify the sources of PII in the system.

Email

Online

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.

PII and PHI is used/collected from existing core applications - SP is not the primary system for data collection. If notification is required, the notification would occur at the point of primary system collection and not at the SP repository level.

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.

PII and PHI may be used from existing core applications. SP is not a publically facing system and is not the primary system of data collection so an option to opt-out does not apply. The method to opt-out would be covered by the core application and the associated PIA.

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

All CMS employees and direct contractors consent to CMS policies regarding appropriate use of CMS technology and the use of employee and contractor credentials to use applications. Additional PII is stored in SharePoint and therefore the process to give notice and obtain consent are controlled by the SORN of the originating 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.

Standard CMS Incident handling Procedures are used if PII/PHI has been inappropriately obtained, used, discussed, or disclosed. If it is inaccurate, the business component or unit within CMS is responsible for editing, correcting, and monitoring it.

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

Integrity - Access managers and site administrators grant access to sites and monitor content.

Availability - daily incremental and weekly full backups are created to ensure content availability.

Accuracy - Users that are granted create/update access can edit and correct content as needed.

Relevancy - Business units/component site administrators are responsible for monitoring content for relevancy.

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

Users:

Users require access to enter and edit data to support CMS business needs, processes, and requirements.

Administrators:

Administrators require access to create new lists, sites, sub-sites, folders, to support business unit requirements.

Developers:

Developers require access as they build and maintain custom applications and workflows to support business requirements and processes.

Contractors:

Direct contractors require access as they build and maintain custom applications and workflows to support business requirements and processes. Direct contractors sign CMS Non- Disclosure Agreements (NDA's).

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

Access managers and system administrators use SharePoint (SP) permissions and permission groups to ensure users only have access to their data and content. Access to content is based on a need-to-know basis.

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.

Access is granted to SharePoint collaboration sites by use of internal SharePoint permissions and groups. These groups are managed by component Access Managers, Site Administrators, and the agency SharePoint support direct contractor - TTC, Inc.

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 employees are required to take the annual CMS security and privacy computer-based training.

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

Access managers have training for managing SP permissions and permission groups to ensure users only update the minimum necessary PII or PHI.

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.

The NARA General Records Schedule DAA GRS-2013-0006-0003 is used stating to "Destroy 1 year (s) after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is appropriate."

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

Data and content is controlled on a need-to- know basis. This is performed by Access Managers and Site Administrators utilizing internal SP permissions and permission groups. SharePoint is an internal intranet (not external facing) application that is only accessible by PIV cards or RSA tokens. Applicable background checks are conducted for all SP users as part of Federal Employee or contractor onboarding processes.

The CMS Baltimore Data Center facility is protected by a variety of physical and environmental controls monitored locally and/or remotely during its 24/7 operation to include security guards monitoring access to doors, cameras, sign in log for visitors and escorts, ID checks, quarterly review of access logs and remote monitoring of environmental and power conditions.