US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/01/2024

OPDIV:

CMS

Name:

CMS SharePoint / CAPMS

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

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.

In January 2016, the Centers for Medicare & Medicaid Services (CMS) Share (SharePoint) and CMS Agency Project Management System (CAPMS) (Project Server) merged into a consolidated hardware platform, hereafter referred to as the Consolidated SharePoint Platform (CSP). In 2020, the decision was made to migrate CMS Share (SharePoint) and CAPMS (Project Server) from the Baltimore Data Center (BDC) to Amazon Web Services (AWS) cloud data center, where it will operate in the CMS Government Enclave.

Therefore, there will be no modification to the underlying server operating system (Microsoft Windows Server 2016) and web application platform (Microsoft SharePoint Server 2016), only to the physical architecture of where the system is housed (AWS Cloud Data Center). There are no deviations from how sensitive data (Personally Identifiable Information) (Protected Health Information) is handled by the system and no additional privacy risks are being introduced.

Describe the purpose of the system.

The Consolidated SharePoint Platform (CSP) solution is an out of the box (OOTB) implementation of Microsoft SharePoint 2016 (CMS SharePoint) and Project Server 2016 (CMS Agency Project Management System) (CAPMS) at CMS. Microsoft SharePoint is an online collaboration platform that runs on Windows Server; Project Server is a project management platform; and both employ Microsoft Structured Query Language (SQL) Server for data storage.

The CSP solution provides support for the following functional use cases: create work products and workspaces, protect confidential documents, provision an organization home page, provision a team site, collaborate on documents, leverage meeting notes, manage and disseminate knowledge, maintain an organization home page, collaborate using a team site, upload and publish video/webcasts, search, and maximize business insights.

The documents stored in CMS SharePoint and CAPMS may consist of standard operating procedures, policy documents, meeting minutes, meeting agendas, helpful notes, and frequently asked questions to support CMS business units and components in effectuating their business processes.

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

Business units and components within CMS may use sensitive information including Personally Identifiable Information (PII) and Protected Health Information (PHI). CMS SharePoint may store the following documents in support of CMS business processes: technical architecture documents, business architecture documents, CMS budget requests, CMS funding reports, contract proposals, vendor proposals, proprietary vendor information, proprietary product information, and human resource documents. Other PII and PHI information that may be uploaded to CMS SharePoint include E-Mail Address, Education Records, Employment Status, Date of Birth, Mailing Address, Financial Account Info, Name, Phone Numbers, and Legal Documents.

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

The Consolidated SharePoint Platform (CSP) solution is an out of the box (OOTB) implementation of Microsoft SharePoint 2016 (CMS SharePoint) and Project Server 2016 (CMS Agency Project Management System) at CMS. Microsoft SharePoint is an online collaboration platform that runs on Windows Server; Project Server is a project management platform; and both employ Microsoft Structured Query Language (SQL) Server for data storage.

The CSP solution provides support for the following functional use cases: create work products and workspaces, protect confidential documents, provision an organization home page, provision a team site, collaborate on documents, leverage meeting notes, manage and disseminate knowledge, maintain an organization home page, collaborate using a team site, upload and publish video/webcasts, search, and maximize business insights.

Personally Identifiable Information (PII) and Protected Health Information (PHI) information that may be uploaded to CMS SharePoint include E-Mail Address, Education Records, Employment Status, Date of Birth, Mailing Address, Financial Account Info, Name, Phone Numbers, and Legal Documents.

Personnel who access or use the system do not use any personal identifiers to retrieve records held in the system.

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

Yes

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

Date of Birth
Name
E-Mail Address
Mailing Address
Phone Numbers
Financial Accounts Info
Legal Documents
Education Records
Employment Status

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?

Personally Identifiable Information (PII) may be used to manage and index CMS SharePoint lists and libraries to provide business owners and system users with the ability to easily organize, filter, and sort documents and content.

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

There are no secondary uses of Personally Identifiable Information (PII).

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

N/A

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
Email
Other
Government Sources
Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A

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.

Personally Identifiable Information (PII) and Protected Health Information (PHI) may be contained in Microsoft Word and Excel documents. If notification of data or content is required, the notification would occur from the business unit responsible for creating the documents.

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.

There is no option to opt-out of the collection of Personally Identifiable Information (PII) and Protected Health Information (PHI). The method to opt-out would be handled by the CMS business unit and business owner.

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 its applications. Personally Identifiable Information (PII) may be stored in CMS SharePoint, and therefore, the process to give notice and obtain consent is controlled by the business owners and users of 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.

Standard CMS Incident Handling Procedures are used if Personally Identifiable Information (PII) and Protected Health Information (PHI) has been inappropriately obtained, used, discussed, or disclosed. If it is inaccurate, the business component or unit within CMS that is responsible for the content 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 their content.

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

Accuracy - Users that are granted access can create, update, and edit 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.

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

Access managers and system administrators use CMS SharePoint permissions and security groups to ensure that users only have access to their respective 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 CMS SharePoint collaboration sites by use of internal CMS SharePoint permissions and security groups. These groups are managed by component Access Managers, Site Administrators, and the Agency SharePoint Team (AST).

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 of the system are required to take the annual CMS Information System Security and Privacy computer-based training.

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

Access managers receive training for managing CMS SharePoint permissions and security groups to ensure that users only update the minimum necessary Personally Identifiable Information (PII) or Protected Health Information (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 and states 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.

The Agency SharePoint Team (AST) holds all administrative access to the servers, CMS SharePoint farm administration sites, and consoles. The AST is given site collection administrator permissions. Site administration access is given out to site owners who own content within their departmental area, based off minimum necessary principles. They are given least privilege access to only be able to manage their site and content.

The users must have an active CMS account to be granted access. The Consolidated SharePoint Platform (CSP) does not store, collect, or maintain access credentials, usernames, or passwords.

CMS SharePoint permissions are granted by CMS employees designated as site owners. The site owner is an individual who has extensive knowledge of SharePoint and the content stored within their CMS SharePoint site. The site owner is required to complete ‘CMS SharePoint: Site Owner’ training course, administered by AST, to obtain the role-based certification. Site owners will have the knowledge necessary to determine who should have access to their documentation and what level of access they should have.

All hardware assets are located in the Amazon Web Services (AWS) data center. Maintenance of the hardware is controlled by AWS support groups. The AWS 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 logs for visitors and escorts, ID checks, review of access logs and remote monitoring of environmental and power conditions. Physical access controls for the AWS Data Center are described in the AWS System Security Plan.

A variety of technical controls are implemented included firewalls, network monitoring and intrusion detection, and multi-factor authentication.