US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/06/2026

OPDIV:

NIH

Name:

SharePoint Platform (SPP)

PIA Unique Identifier:

P-3392404-353773

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

The SharePoint Platform (SPP) is a subsystem of the NIH Office of Research Services (ORS) and Office of Research Facilities (ORF) General Environment Moderate (OGEM). The SPP is a collection of websites and applications hosted on the Enterprise Network Services (ENS) and SharePoint 2019, developed to meet the business needs of the NIH community. These components are grouped by their functional purpose and collectively ensure efficient, secure, and responsive support for both public and NIH internal stakeholders. Due to format character limitations, additional pages are included with details.

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

SPP collects, stores, and may share information, including personally identifiable information (PII) as required to provide these services. The informational components that do not collect PII are: Division of Emergency Management (DEM), Division of Occupational Health and Safety (DOHS)-Automated External Defibrillator (AED), Office of Research Services (ORS)–News2Use, Salud, Office of Administrative Management (OAM) Intranet Site and Posted Space App. See additional pages for

reference of all the components that collect PII grouped by category type.

Those using this system login or their credentials are being leveraged by the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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

The SPP is a subsystem of the NIH ORS and ORF OGEM. The SPP is a collection of websites and applications hosted on the ENS and SharePoint 2019, developed to meet the business needs of the NIH community. These components are grouped by their functional purpose and collectively ensure efficient, secure, and responsive support for both public and NIH internal stakeholders. Due to format character limitations, additional pages are included with details.

SPP collects, stores, and may share information, including PII as required to provide these services. The informational components that do not collect PII are DEM, DOHS-AED, ORS–News2Use, Salud, OAM Intranet Site, Posted Space App. See additional pages for reference of all the components that collect PII grouped by category type.

Those using this system login or their credentials are being leveraged the IAM Services which maintains its own unique PIA on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

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

Yes

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

Name
Photographic Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Financial Accounts Info
Education Records
Employment Status
Position Title, Calendar leave dates, Biography, Expertise, Username, Passwords, Age, School grade
Visitor Internet Protocol (IP) address, Device identifiers, Personal Identity Verification (PIV) card number, badge number/expiration
Event/activity registration details, tracking number, request date, event date/time
Branch/Division/Department/Institute/Center/Facility name, Building, room, site, campus locations, Project Identification (ID), tour of duty, conference/workspace reservation/ approval, WR#
Common Accounting Number (CAN), Company names, Invoice and purchase order number, Drug Enforcement Agency (DEA) registration number/expiration

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

Employees
Public Citizens

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The primary purpose of collecting PII is for access to services such as NIH parking and transportation, building design and review, veterinary services, art and conference services, etc.

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

Software development and testing, problem resolution

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

5 U.S.C. 7901; 5 U.S.C. 301 and 302; 44 U.S.C. 3101 and 3102, 5 U.S.C. 301 and 302, E.O. 10450, 42 U.S.C. 203, 282

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

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

SORN: 09-25-0216, Administration: NIH Electronic Directory, HHS/NIH

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Online
Government Sources
Within OpDiv
Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

An OMB information collection approval is not required for federal employees. Information that is collected from public citizens on the Contact Us link is exempt because the information is used solely to self identify and request services.

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.

Those entering the system will see a privacy notice on the initial banner which links to the NIH privacy statement.

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 within the SharePoint Platform can be collected via authorized/approved system-to-system methods, via individual informed surveys/interviews or via direct/optional submission by individual employees.

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

In the event of major changes related to PII in the system, the System Owner in coordination with Business Owner and IC ISSO will initiate communication with ORS Privacy Office. Notification and consent will be obtained from affected individuals via text, email, and telephone.

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.

For individuals concerned that their PII has been inappropriately obtained, used, disclosed, or is inaccurate, please contact the System Owner, Jennifer Phan via email at jennifer.phan@nih.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.

Periodic reviews are conducted by the Information System Security Officer (ISSO) / Office of Innovation and Information Technology (OIIT) Security to validate the system's security posture.

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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

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 to PII is assigned to personnel based upon current job responsibilities. A NIH IAM Systems account login is required to gain access to the stored PII data.

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.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials. Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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

NIH system administrator training and internal (OIIT Security) system owner training is available for technical personnel.

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.

Records are retained and disposed of under the authority of the NIH Records Retention Schedule. Item 09-201: Facility, space, vehicle, equipment, stock, and supply administrative and operational records. Facility, space, vehicle, equipment, stock, and supply administrative and operational

records.
Description: Records relating to administering and operating facilities, spaces, Federally owned and operated housing, land vehicles, water vessels, equipment, stocks, and supplies.
Disposition Destroy when 3 years old or 3 years after superseded or obsolete, whichever is applicable. Longer retention is authorized for business use. DAA-GRS-2016-0011-0001
Item 09-207: Facility, space, and equipment inspection, maintenance, and service records. Records tracking completion of custodial and minor repair work.
Description: Facility, space, and equipment inspection, maintenance, and service records. Records documenting facility structure and long-term maintenance.
Records documenting inspection, maintenance, service, and repair activities relating to buildings, grounds, Federally owned and operated housing, equipment, and personal property.
Disposition: Destroy when 90 days old, but longer retention is authorized if required for business use. DAA-GRS-2016-0011-0009
Item 09-302: Mail, printing, and telecommunication services administrative and operational records. Records of internal mail room, printing/duplication services, and radio/telecommunication services administration and operation.
Description: Mail, printing, and telecommunication services administrative and operational records. Records of internal mail room, printing/duplication services, and radio/telecommunication services administration and operation.
Disposition: Destroy when 3 years old, or 3 years after applicable agreement expires or is canceled, as appropriate, but longer retention is authorized if required for business use. DAA-GRS-2016-0012-0001

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

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.

Physical Controls: The information technology (IT) hardware used to host protected information is located in a secured data center facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.