

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/27/2024

OPDIV:

NIH

Name:

NCCIH SharePoint

PIA Unique Identifier:

P-5658862-677296

The subject of this PIA is which of the following?

Minor Application (child)

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?

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.

This validation is intended to refresh content and correct the system name throughout. Removed instances of "External SharePoint" where the system name is "SharePoint".

Describe the purpose of the system.

The National Center for Complementary and Integrative Health (NCCIH) SharePoint Workspace is a central collaboration web site used internally to post information and facilitate communication between work groups, offices/divisions, and senior staff. The SharePoint site centralizes information so that the correct data or document is shared, reviewed, and/or revised. Features include automatic alerts, task assignment with e-mail notifications, and discussion boards.

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

NCCIH SharePoint does not collect personally identifiable information (PII), but interfaces with other government systems to import new hire contact information, grant application and management

information. The system stores grant applications from NIH's eRA and grant progress reports and summary statements from NIH's Query/View/Report (QVR) system, both of which maintain their own unique privacy impact assessments (PIAs).

NCCIH uses contact information from these sources, including name, email address, phone number, and mailing address to contact new hires, principal investigators, and other institution personnel at universities and research hospitals.

NIH eRA and QVR-sourced data contain names and institutional contact data (mailing address, phone, and email) for study personnel. Grant applications frequently contain resumes and curriculum vitae (CV) of study personnel, that contain educational and employment histories. Some grant applications may contain the last 4 digits of study personnel social security numbers, but NIH doesn't solicit this data, and its presence is inadvertent and incidental.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 collects unique user credentials and stores them in an encrypted format. The IAM Service is an essential service which facilitates and governs network access to various resources.

eRA is a system name, not an acronym.

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

The NCCIH SharePoint Workspace is a central collaboration web site used internally to post information and facilitate communication between work groups, offices/divisions, and senior staff. The SharePoint site centralizes information so that the correct data or document is shared, reviewed, and/or revised. Features include automatic alerts, task assignment with e-mail notifications, and discussion boards.

NCCIH SharePoint does not collect PII, but interfaces with other government system to import new hire contact information, grant application and management information. The system stores grant applications from NIH's eRA and grant progress reports and summary statements from NIH's QVR system, both of which maintain their own unique PIAs.

NCCIH uses contact information from these sources, including names, email addressed, phone numbers, and mailing addresses to contact new hires, principal investigators, and other institution personnel at universities and research hospitals. NIH eRA and QVR-sourced data contain names and institutional contact data (mailing address, phone, and email) for study personnel. Grant applications frequently contain resumes and CV of study personnel, that contain educational and employment histories. Some grant applications may contain the last 4 digits of study personnel social security numbers, but NIH doesn't solicit this data, and its presence is inadvertent and incidental.

Those requiring access to this system log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

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
Education Records
Employment Status
Resume/CV

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

New Hires: NCCIH Administrative Officers use job applicant's PII to contact the applicant prior to hire and establishment of an NIH email account. OR

NCCIH AO copy the new-hire's personal email address from SP during the on-boarding process

Grants Management: The Division of Extramural Research uses the Principal Investigators' PII to contact PIs at all stages of the grant management life-cycle.

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.

The legal authority to collect grant applicant information and maintain this system is based upon the data's source system, eRA:

5.U.S.C. 301; 42 U.S.C. 217a, 241, 242, 281, 282, 284, 284a, 285, 285b, 285c, 285d, 285e, 285f, 285g, 285h, 285i, 285j, 285k, 285l, 285m, 285n, 285o, 285p, 285q, 285r, 285s, 285t, 286, 287, 287b, 287c-11, 287c-21, 287d, 288, 44 U.S.C. 3101, 35 U.S.C. 200-212, 48 CFR Subpart 15.3, and 37 CFR 401.1-16.

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.

OPM/GOVT-1: General Personnel Records.

09-25-0036: Extramural Awards and Chartered Advisory Committees (IMPAC 2), Contract

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Identify the OMB information collection approval number and expiration date

NCCIH SharePoint is not involved in the initial PII collection and is not an authoritative PII repository. Any such notifications occur at the source systems: USAJobs, NIH's eRA, and QVR system, which maintain their own unique PIAs. .

Grant applications stored in NCCIH SharePoint are covered by the Standard Form (SF) 424's Office of Management and Budget (OMB) Number: 4040-0004; Expiration Date: 11/30/2025.

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.

Employment applicants submit their personal contact information, educational and employment histories in Office of Management and Budget's (OMB's) USAJobs system which maintains its own unique PIA. Hiring managers download relevant resumes from USAJobs and upload them to NCCIH SharePoint for consideration.

Other PII-containing documents within SharePoint, like the Standard Form (SF) 424 and Progress Reports are sourced from NIH's eRA and QVR system, both of which maintain their own unique PIAs.

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.

NCCIH SharePoint is not involved in the initial PII collection and is not an authoritative PII repository. Any such notifications occur at the source systems: USAJobs, NIH's eRA, and QVR system, which maintain their own unique PIAs. Questions or concerns for opting out of collection should be directed to the source system business owner.

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

There is no Institute/Center/Office (ICO)-level notification or consent process. NCCIH SharePoint is not involved in the initial PII collection and is not an authoritative PII repository. Any such notifications occur from the source systems: USAJobs, NIH's eRA, and QVR system, which maintain their own unique PIAs.

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.

Grantees may contact their Program Officer to update their contact information if necessary. However, NCCIH SharePoint is not an authoritative PII repository. Principal Investigators and job applicants submit their PII to source systems: USAJobs and NIH's eRA and QVR system maintain their own unique PIAs.

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 to periodically review PII. NCCIH SharePoint primarily uses Grant identifications (IDs) as search keys. NCCIH SharePoint is not an authoritative repository for any PII. Grantees' contact information exist on other online directories for contact purposes. PII for job

applicants will have either resulted in employment or will be archived. NCCIH performs annual and semi-annual records management weeks to expunge data.

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.

NCCIH SharePoint sub-siteowners notify the SharePoint administrators to add new users and set their permissions at account creation time. Administrators assign users to groups, and the groups have access to resources.

The Administrators have access to all site content, for troubleshooting purposes.

Administrators are also developers who may access PII in on-premises development, staging, and production environments, managed by the NIH Center for Information Technology (CIT).

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.

NCCIH SharePoint Administrators use SharePoint security groups for centralized management of groups and security. A SharePoint group is a set of individual users and can also include NIH IAM Services Domain Services groups. Each SharePoint sub-site has independent site and library permissions.

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 and privacy awareness training. Training is completed on the <http://irtsectraining.nih.gov> site with valid NIH credentials.

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

NCCIH SharePoint administrators must complete the annual HHS Information Technology (IT) Administrator's course or equivalent external training. NCCIH SharePoint developers must complete the National Library of Medicine (NLM) Application Security Checklist & Best Practices for Developers or equivalent external training annually.

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 maintained within NCCIH SharePoint. Records are retained and disposed of under the authority of the NIH Records Retention Schedule.

Item 07-204 System access records; Systems requiring special accountability for access; These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Disposition: Destroy 6 years after password is altered or user account is terminated, but longer

retention is authorized if required for business use. DAA-GRS-2013-0006-0004

Item 02-004: Extramural program and grants management oversight records

These records are generated during the administration and execution of extramural program activities.

Disposition: Cut off annually. Destroy 3 years after cutoff. DAA-0443-2013-0004-0004

Item 02-005: Official Case Files of Applications and Awards, Appeals, and Litigation Records for Grants, Cooperative Agreements, and Other Transaction Activities

Official case files of funded and unfunded grants and cooperative agreements, award applications, and appeals and litigation records. Records also include those supporting other transaction awards and activities.

Disposition: Cut off annually following completion of final award-related activity that represents closing of the case file. Destroy 30 year(s) after cutoff. DAA-0443-2019-0008-0001

Item 06-109- Job Application Packages.

Job application packages. Application packages for competitive positions, in USAJobs or its successors, and other systems, whether electronic or analog

Disposition: Destroy 1 year after date of submission. DAA-GRS-2014-0002-0011

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

Administrative Controls: All NCCIH SharePoint users, administrators, developers, and direct contractors are government agency-badged personnel. All personnel have taken mandatory annual security and privacy training classes. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data. NIH Data Protection performs a quarterly DLP (Data Loss Prevention) scan, searching for Social Security Numbers, Credit Card Numbers, and Medical Records Numbers. The NCCIH ISSOs review these scans to ensure NCCIHESP is only collecting the minimum necessary PII.

Physical Controls: The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room. The SharePoint system is electronically behind the NIH firewall and can only be accessed from behind the firewall. The information is physically secured by a required key card and employee badge and electronically secured by a password login procedure to the NIH computer system, and a requirement of a password when accessing the database. A comprehensive Incident Response Plan is also maintained. Information is also secured by least privilege, separation of duties, an intrusion detection system, locks and background investigations.

