

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/27/2024

OPDIV:

NIH

Name:

NCCIH Local Network: NCCIH External SharePoint

PIA Unique Identifier:

P-7081689-149163

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.

Added the new National Institutes of Health, National Center for Complementary and Integrative Health (NCCIH) External SharePoint (ESP) (NCCIHESP) Mission/Purpose. The new statement reflects the inactivation of the Pain Management Collaboratory Initiative (PMCI) and the In-Progress Review (IPR) modules.

NCCIH has stopped actively sharing the Pain Management Collaboratory Implementation (PMCI) and In Progress Reviews (IPR) information but must maintain that data until NIH Records Retention authorizes its disposal.

NIH Data Protection Data Loss Prevention scans have been incorporated in order to search for unintentional personally identifiable information (PII).

Describe the purpose of the system.

The NIH National Center for Complementary and Integrative Health (NCCIH) External SharePoint (ESP) (NCCIHESP) is an external facing website that supports the Office of Clinical and Regulatory Affairs (OCRA), a division of NCCIH responsible for planning, coordinating and monitoring clinical trials. NCCIHESP facilitates the collection of Accrual Reports from external Investigators (i.e., outside of NIH).

NCCIHESP's capabilities includes

- 1) automating the collection of Accrual Reports from external Investigators; and
- 2) the ability to generate reports to maximize the Accrual Report Tracking.

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

NCCIH External SharePoint directly collects clinical study participant accrual progress reports and grant review comments and feedback, including names and email addresses. In addition, 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). 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, of which may 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.

The SharePoint search functions do not index the content of files and therefore cannot search by personally identifiable information (PII) fields. NCCIH External SharePoint is not an authoritative repository for any PII. Grantees and work group participants are listed on other online directories for contact purposes.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique 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.

NCCIHESP is an external facing website that supports the OCRA, a division of NCCIH responsible for planning, coordinating and monitoring clinical trials. NCCIHESP facilitates the collection of Accrual Reports from external Investigators (i.e., outside of NIH). NCCIHESP's capabilities include: 1) automating the collection of Accrual Reports from external Investigators; and 2) the ability to generate reports to maximize the Accrual Report Tracking.

NCCIH External SharePoint directly collects non-sensitive clinical study participant accrual progress reports and grant review comments and feedback: including names and emails. In addition, 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. 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, of which may 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
Resumes and Curriculum vitae (CV)

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

Employees
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?

Accrual Reports: NCCIH personnel reference Principal Investigators' name to verify that the submitted accrual reports correlate to the listed grant identifications (IDs). If the Principal Investigator submits an email address, a confirmation can be sent.

In-Progress Reviews (IPR): (Note: NCCIH stopped IPR reviews after 2018. NCCIH is adding zero new IPR-related data. NCCIH must maintain the existing records for ten years, per the NIH General Records Schedule.) Any PII in the standard form (SF) 424 grant applications is inadvertent and incidental. The NIH, Department of Defense (DOD), and Veterans Administration (VA) reviewers do not use PII in consideration of study progress.

Pain Management Collaboratory Implementation Team (PMCIT) (Note: NCCIH stopped hosting the PMCI after 2018. NCCIH is not adding any new PMCI-related data. NCCIH must maintain the existing records for ten years, per the NIH Records Schedule. Members use the rosters to contact each other.

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 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?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Online

Identify the OMB information collection approval number and expiration date

With HHS OpDiv 4040-0004. Expiration Date: 11/30/2025

Other HHS OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

NCCIH External SharePoint lacks any downstream machine-to-machine interfaces.

Information is shared via access to the External SharePoint site. User behavior is governed by their respective agencies' Rules of Behavior and Non-Disclosure Agreements.

Describe the procedures for accounting for disclosures.

Audit logs are be used to disclose what information is shared and tracked outside of HHS.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

NCCIH's Office of Clinical and Regulatory Affairs directs grantees to this website specifically to submit accrual reports for existing grants. Grantees obtain the sample template that contains the data fields from a publicly accessible website: [https://nccih.nih.gov/grants/policies/SARP- template](https://nccih.nih.gov/grants/policies/SARP-template)

Other PII-containing documents within External SharePoint, like the 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.

Principal Investigator Name submission is required for accrual reports. The email address field only appears if the Principal Investigator opts-in by clicking the "Send me a confirmation e-mail" checkbox. If an individual chooses to opt out of providing their PII, they don't have access to the system. PII derived from NIH eRA is covered under its own unique PIA.

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. If an individual chooses not to provide PII, they don't access the system. PII for reporting purposes is submitted within documents to NIH's eRA and QVR system, both of 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.

There is no process in place. If an individual chooses not to provide PII, they don't access the system. PII for reporting purposes is submitted within documents to NIH's eRA and QVR system, both of which maintain their own unique PIAs and should be addressed with those system owners.

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. The SharePoint search functions do not index the content of files and therefore cannot search by PII fields. NCCIH External SharePoint is not an authoritative repository for any PII. Grantees and work group participants are listed on other online directories for contact purposes.

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 External SharePoint sub-site owners notify the SharePoint administrator 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. The Center for Information Technology (CIT) creates an on-premises staging environment to redact PII and sensitive data before developers export it for development testing.

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 External SharePoint Administrators use SharePoint security groups for centralized management of groups and security. 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.

HHS, DoD, and VA personnel must complete their respective organizations' annual Federal Information Processing Standards (FISMA) -mandated security and privacy awareness training to obtain access to the NIH systems.

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

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

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 02-004 - Extramural Program and Grants Management Oversight Records

These records are generated during the administration and execution of extramural program activities. This schedule item is intended to capture all extramural program and grants management records that are not part of an official case file (Item 0001 or 0002) or animal welfare assurance file (Item 0003). These records support the operations, compliance, reporting, and oversight functions of the NIH Extramural Program and the financing of research endeavors with the purpose of ensuring scientific integrity and public accountability of the NIH extramural research portfolio. Extramural program and grants management oversight records are consolidated under one common temporary retention item.

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

Item 07-201 - Systems and data security records.

These are records related to maintaining the security of information technology (IT) systems and data. Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific systems for which they were written. This series also includes analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses.

Disposition: Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. DAA-GRS-2013-0006-0001

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.

Exclusion 1. Excludes records relating to electronic signatures.

Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.

Systems requiring special accountability for access.

These are user identification records associated with systems which are highly sensitive and potentially vulnerable.

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

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

Administrative Controls: All NCCIH External SharePoint users, administrators, developers, and direct contractors are government agency-badged personnel, subject to their own agency's rules of behavior and training requirements.

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) scans. The NCCIH Information System Security Officer (ISSO) reviews these scans to ensure NCCIHESP is only collecting the minimum necessary PII.

Physical Controls: The servers reside in the 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.