US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/09/2025

OPDIV:

NIH

Name:

Clinical Collaboration System (NCCS) Huddle

PIA Unique Identifier:

P-6621446-159278

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?

Yes

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.

Not Applicable (N/A)

Describe the purpose of the system.

The National Institute of Allergy and Infectious Diseases (NIAID) Clinical Collaboration System (NCCS) Huddle is a Software as a Service (SaaS). Huddle provides cloud based online collaboration and document sharing solutions for businesses. Using a SaaS model, Huddle combines Enterprise Content Management (ECM) and social software allowing NIAID to collaborate flexibly both internally and externally. The key functionality of the Huddle system is a web-based workspace in which NIAID users can use hierarchical file storage with document preview. Permission models are in place to allow for restrictions of documents to specific teams with dashboards being used to provide team activity overview. NIAID is currently using Huddle to conduct remote monitoring visits for multiple trials, register sites for the INSIGHT trials, and to upload study-specific documents for Quality Control. INSIGHT is the name of the partnering entity that works with NIAID to complete clinical

trials.

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

The information types collected include: name, email, phone number, education records, mailing address, Lab certification information, Statement of Investigator (form FDA 1572) clinical trial forms, Curriculum vitae (CVs), medical records, medical notes, Biometric Identifiers.

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

The National Institute of Allergy and Infectious Diseases (NIAID) Clinical Collaboration System (NCCS) Huddle is a Software as a Service (SaaS). Huddle provides cloud based online collaboration and document sharing solutions for businesses. Using a SaaS model, Huddle combines Enterprise Content Management (ECM) and social software allowing NIAID to collaborate flexibly both internally and externally. The key functionality of the Huddle system is a web-based workspace in which NIAID users can use hierarchical file storage with document preview. Permission models are in place to allow for restrictions of documents to specific teams
with dashboards being used to provide team activity overview. NIAID is currently using Huddle to conduct remote monitoring visits for multiple trials, register sites for the INSIGHT trials, and
to upload study-specific documents for Quality Control.

The information types collected include: name, date of birth, email, phone number, photographic identifiers, education records, mailing address, Lab certification information, Statement of Investigator (form FDA (Food and Drug Administration) 1572) clinical trial forms, Curriculum vitae (CVs), medical records, medical notes, Biometric Identifiers.

Users log in to this system using 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.

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
Photographic Identifiers
Biometric Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Education Records
Lab certification information, FDA 1572s, and Curriculum vitae(CVs)

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

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

PII is used for identification of the users within the system. Email address is also required in order to send notifications. Other PII (phone number and mailing address) is stored within the system, but not used by the system.

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

PII stored in this application is used in the performance of clinical trails managed by the Division of Clinical Research (DCR).

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

5 U.S.C 301 and 302

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.

09-25-0115, Administration: Curricula Vitae of Consultants and Clinical Investigators

09-25-0099, Clinical Research: Patient Medical Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Within the OPDIV
Non-Governmental Sources
Other

Identify the OMB information collection approval number and expiration date

Not Applicable (N/A). The collection of the information that is put into NCCS occurs well before it is actually entered. The system is not the instrument that directly collects the information, only that the file packages that are stored and uploaded to NCCS as part of daily operations. Those activities occur by clinical contractors and Federal personnel.

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.

Informed consent is obtained for all participants of the studies, and users of Huddle are aware that their emails and names are collected for account purposes.

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.

A user is required to provide their first, last, and display names as well as their primary email address during the registration process. If this information is not provided, the user will be unable to use Huddle.

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

The business owner of NCCS is responsible for notifying and obtaining consent of individuals whose PII may be impacted when major changes occur.

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.

Individuals with concern about or updates of their PII always have the ability to contact the NCCS Help Desk, which will address their concerns or make requested changes.

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

The business owner of the application or repository is responsible for periodic reviews of Personally Identifiable Information (PII) in NCCS to ensure the data's integrity, availability, accuracy and 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.

Only specific personnel have access to the PII and appropriate management approval is required prior to access. Access to PII is limited to the NCCS Engineers and NCCS Customer Services groups. The managed policy and process around access control are documented in the NCCS Access Control Policy Doc ID 10006.

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.

For applications and repositories with PII data about NIAID employees, only a pre-authorized group of users with the need to access information about an employee has access to the PII.

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 and contractors undertake the NCCS Information Security training which encompasses privacy of data.

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

When a user is given authorization to NCCS, the business owner ensures that each user is trained, including access controls and restrictions.

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.

Login /Systems Access Records are retained and disposed of under the authority of the (NIH General Records Schedule, Section 3.2.030: System Access Records.) These are temporary

records. Destroy when business use ceases.
[Disposition Authority: DAA-GRS-2013-0006-0003]

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

Administrative Controls - The Huddle tenant is broken up into workspaces and files within those workspaces. All non-privileged Users are provided with the type of access specified and granted by the customer. Privileged Users within the Huddle account have access to the profiles all users within the Huddle tenant. User accounts are only granted to external users if the external user is explicitly invited by the customer to the Huddle tenant and assigned access rights to their workspace's contents. The Huddle Databases are only accessible to the Huddle privileged administrators as part of the role-assignment of privileged.

Technical Controls - The Huddle tenant is broken up into workspaces and files within those workspaces. All non-privileged Users are provided with the type of access specified and granted by the customer. Privileged Users within the Huddle account have access to the profiles all users within the Huddle tenant. User accounts are only granted to external users if the external user is explicitly invited by the customer to the Huddle tenant and assigned access rights to their workspace's contents. The Huddle Databases are only accessible to the Huddle privileged administrators as part of the role-assignment of privileged.

Physical controls - the Huddle tenant is a Software-as-a-Service (SaaS) virtual system that does not have any physical system components.

Identify the publicly-available URL:

niaid.huddle.com

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No