# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

02/18/2025

### OPDIV:

NIH

### Name:

NIMH Cogmood Application

**PIA Unique Identifier:**

P-7980888-641336

**The subject of this PIA is which of the following?**

Electronic Information Collection

**Identify the Enterprise Performance Lifecycle Phase of the system.**

Development

**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.**

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 National Institutes of Mental Health (NIMH) Cogmood Application is a website developed by the NIMH Learning Machine Core Center where research participants respond to surveys about their mental health symptoms and download cognitive tasks which they run on their own computers. These tasks upload data on task performance to our website. The information is collected in connection with research on depression, anxiety, and Attention Deficit Hyperactivity Disorder (ADHD).

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

The NIMH Cogmood Application collects research participants' race, ethnicity, sex, age at birth, current age, answers to questions about their mental health symptoms, responses to cognitive tasks and worker identifications (IDs). The server hosting the Cogmood application also stores NIMH Machine Learning Core (MLC) staff usernames and hashes in order to confirm application specific passwords.

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

Research participants are recruited on a Participant Management Platform (PMP) outside and not connected to NIMH Cogmood Application. The PMP presents participants with a link to the Cogmood Application along with a short description of the surveys and tasks they will be asked to complete. That link includes their PMP specific Worker ID information. Clicking on that link brings the participants to the Cogmood Application. As soon as they reach the Cogmood Application, an encrypted session cookie containing their Worker ID is stored in the participant's browser. This cookie allows participants to resume participation if they are interrupted. It also prevents participants from abusing the application by attempting to complete it with multiple Worker IDs. If they agree to the consent form, they proceed to the survey collection. Survey responses are stored with a randomly assigned ID. The link between this random ID and Worker IDs is stored in a separate file on the server hosting the Cogmood Application. Once participants complete the surveys, they download and run a program which runs a set of cognitive tasks on their personal computers. As the participants complete the tasks, the program running the tasks automatically uploads their responses to the server, identified by their Worker ID. The tasks will not run if the program is unable to communicate with the Cogmood Application. Once participants have completed the survey and tasks, they are redirected to the PMP with a code identifying what proportion of the survey and task they completed for payment purposes.

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

Yes

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

Worker ID, Random ID
Payment code
Race, ethnicity, sex, age at birth, current age
Username and password

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

Employees
Public Citizens
Consented Research Participants

**How many individuals' PII is in the system?**

500-4,999

**For what primary purpose is the PII used?**

PII is used to identify participants and NIMH staff.

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

No other uses

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

42 USC § 285p, PL84-182

**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.**

09-25-0200: Clinical, Basic and Population-based Research Studies of the National Institutes of

**Identify the sources of PII in the system.**

Directly from an individual about whom the information pertains

Online

**Identify the OMB information collection approval number and expiration date**

Q23a-N/A. Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

**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.**

Participants read a notice in the description of the study in the PMP, where it's stated their Worker ID will be collected and used in the NIMH Cogmood Application. When the participants enters into the NIMH Cogmood Application, they will have to sign an informed consent form that provide additional details about the collection of personally identifiable information (PII), before completing their surveys and tasks. NIMH MLC Staff opt in when they agree to become administrators for the NIMH Cogmood Application

**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.**

Participants can opt-out of data collection by declining to click the link on the PMP that will bring them to the Cogmood Application. They will not be able to participate in the study if they decline to click the link. NIMH MLC staff are not required to become administrators of the Cogmood Application. They may opt-out of having their user IDs stored on the server by declining to become administrators.

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

A notification is posted in the study description in the PMP to obtain additional consent. Information from participants that do not sign the new consent, will not be able to participate in future studies. NIMH staff will be notified via email.

**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.**

Contact information for the principal investigator of the study is included in the consent form and participants receive a copy of it. If the participant has any concerns they are encouraged to reach out directly. Participants may also send a message through the PMP. NIMH staff can contact the NIMH Information Systems Security Officer (ISSO) at isso@nimh.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.**

There is no process in place for periodic review of participants PII because it will be removed manually by administrators at least once every two weeks from the server hosting the Cogmood Application.

**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 roles are granted by program managers only for information/data pertinent to the user role.

**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.**

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.

**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).**

Users receive system training conducted by program manager or development team.

**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 Records Schedule System.
Item 01-003 - Records of All Other Intramural Research Projects. Cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer.
Disposition: Destroy 7 years after cutoff in accordance with the National Archives and Records Administration (NARA) approved disposition schedule.
Disposition Authority: DAA-0443-2012-0007-0003.

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

Administrative safeguards: NIH staff, including direct contractors take mandatory security and privacy training and include system security and contingency plan. Access is via least privilege through role-based access, and policies for retention and destruction of PII are in place. 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. Files are backed up regularly and stored offsite. Contract clauses ensure adherence to privacy provisions and practices.

Physical Safeguards: Physical access to the system is controlled by security guards, employee badging, proximity cards, card readers, and security cameras. Access to the server is controlled by card readers at the server room door. There is a battery backup for power until the backup generator starts. Fire protection including sprinklers, and flooding sensors at the floor level.

Technical Controls: Technical Safeguards include restricting files using secure socket layer encryption, a two-factor authentication and role-based access controls.

**Identify the publicly-available URL:**

mlc.nimh.nih.gov/cogmood. Note that attempting to access this website without a Worker ID encoded in the URL parameter will result in redirection to an error page. In this case, no PII is captured by the website.

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?**

No

**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