US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/05/2025

OPDIV:

NIH

Name:

NHLBI Chat

PIA Unique Identifier:

P-8368884-565628

The subject of this PIA is which of the following?

Major Application

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.

Alteration in Character of Data

Describe in further detail any changes to the system that have occurred since the last PIA.

The National Heart, Lung, and Blood Institute (NHLBI) is updating this PIA to evaluate privacy risks from two new NHLBI Chat capabilities.

1) The system now allows the use of Personally Identifiable Information (PII), excluding Social Security Numbers (SSNs), Employer Identification Numbers (EINs), and Taxpayer Identification Numbers (TINs). Previously, users were not allowed to upload any PII. Data Loss Prevention (DLP) rules were in place to prevent users from entering in any PII. Now, the DLP rules are being modified to prohibit only SSN/EIN/TIN from being entered; all other PII will be allowed. Any PII entered will be stored and may be used for retrieval of data. This includes potential PII from public citizens, business partners, vendors/suppliers, and patients.

2) Implementation of chat deletion functionality. Current functionality retains chat records infinitely. With this new PIA, chat records will be maintained with the system, as follows:

a) Soft-delete after 90 days. Unused chats will disappear from a user’s list.

b) Hard-delete after 90 more days (180 total). The chat will be fully deleted from the database.

Describe the purpose of the system.

National Heart, Lung, and Blood Institute (NHLBI) Chat is a web browser-based internal chatbot powered by artificial intelligence (AI) available and limited only to all NHLBI staff. NHLBI Chat enables NHLBI staff to use generative AI for their day-to-day work. Current known uses cases are:

1) Drafting and Editing: staff can use NHLBI Chat to draft and refine emails, memos, and other working documents to improve clarity and communication.
2) Brainstorming: staff can use NHLBI Chat to refine project ideas, develop research plans, and contemplate strategic plans
3) Programming: staff use the tool to write and troubleshoot code, such as Python, R, excel, and other languages
4) General Technical support: NHLBI Chat helps staff with general technology questions as an alternate to searching on-line.

NHLBI Chat can analyze text or images and can generate text or images. The tool cannot analyze or generate other types of content, such as videos, music, or sound. All exchanges are tracked in a database hosted on the server.

The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.

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

NHLBI Chat allows users to enter free-text input, which may contain personally identifiable information (PII) depending on what they choose to share during their interactions with the chat. Data Loss Prevention (DLP) rules prohibit entering Social Security Numbers (SSNs), Employer Identification Numbers (EINs), and Taxpayer Identification Numbers (TINs); all other PII is allowed. Users are also advised against including information shared without consent.

Depending on how the chat is used, free-text-input may include PII (excluding SSN/EIN/TIN) relevant to specific user needs or scenarios such as the following:
1) Patient Medical Information
If patients' medical histories are entered for analysis or review, this may include details like names, mother's maiden name, contact information (email address, phone numbers, etc.), birth dates, medical record numbers, health conditions, medical notes, financial account information, race, religion, sex, birth locations, photographic and biometric identifiers
2) Staff/Contractor Administrative Information
For drafting documents like staff renewals, performance evaluations, travel forms, hiring memos, contract staff on-boarding and clearance etc., details may be included such as: names, contact information (email address, phone numbers, etc.), certificates, education records, foreign activities, employment status, legal documents, device identifiers, passport number, age, sex, military status.
3) Vendor Information
If entering vendor information for procurement and purchasing purposes, data like vendor names, emails, phone numbers, mailing addresses, certificates, driver's license numbers, vehicle identifiers, financial account information may be stored.
4) Grant Research Information
When assigning grants to departments, analyzing research data management plans, and tracking research components, investigator details like names, contact information, affiliated institutions may be stored.
5) Survey Response Information
For survey analysis, participant information like names, emails, phone numbers may be stored.
6) NHLBI Chat user data
For archiving and retrieval purposes, NHLBI Chat collects and stores the user's data including the

username, email, and user's NIH ID. Additionally, hiring and/or contracting documentation may include data like license number, photographic identifiers, passport number, and other information related to employment/contracting purposes.

NHLBI Chat has free text capabilities which allows potentially other PII entries. Nonetheless, the user must agree to certain terms and conditions before using the tool. Those terms include the following guidelines: "Entering SSN, EIN or other Taxpayer ID is not allowed. Please ensure any PII entered does not include SSN/EIN/TIN. Please ensure any PII entered into NHLBI Chat is deemed absolutely necessary and to the best of your knowledge, permission to use this PII has been obtained separately from the impacted person(s)."

NHLBI Chat is accessed behind the NIH firewall using the secure sign-on Personal Identity Verification (PIV) through the NIH Identity, Credential, and Access Management (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.

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

National Heart, Lung, and Blood Institute (NHLBI) Chat is a web browser-based internal chatbot powered by artificial intelligence (AI) available and limited only to all NHLBI staff. NHLBI Chat enables NHLBI staff to use generative AI for their day-to-day work. Most common general uses cases include the following, but this list should not be considered exhaustive.

1) Drafting and Editing: staff can use NHLBI Chat to draft and refine emails, memos, and other working documents to improve clarity and communication.
2) Brainstorming: staff can use NHLBI Chat to refine project ideas, develop research plans, and contemplate strategic plans
3) Programming: staff use the tool to write and troubleshoot code, such as Python, R, excel, and other languages
4) General Technical support: NHLBI Chat helps staff with general technology questions as an alternate to googling.

NHLBI Chat can analyze text or images and can generate text or images. The tool cannot analyze or generate other types of content, such as videos, music, or sound. All exchanges are tracked in a database hosted on the server.

Depending on how the chat is used, free-text-input may include PII (excluding SSN/EIN/TIN) relevant to specific NHLBI user needs or scenarios such as the following:

1) Patient Medical Information
If patients' medical histories are entered for analysis or review, this may include details like names, mother's maiden name, contact information (e.g., email address and phone number), birth dates, medical record numbers, health conditions, medical notes, financial account infomation, race, religion, sex, birth locations, photographic and biometric identifiers.

2) Staff/Contractor Administrative Information
For drafting documents related to staff renewals, performance evaluations, travel forms, hiring memos, contract staff on-boarding and clearance, details may be included such as: names, contact

information (e.g., email address and phone number), certificates, education records, foreign activities, employment status, legal documents, device identifiers, passport number, age, sex, military status.

3) Vendor Information
If entering vendor information for procurement and purchasing purposes, data like vendor names, emails, phone numbers, mailing addresses, certificates, driver's license numbers, vehicle identifiers, financial account information may be stored.

4) Grant Research Information
When assigning grants to departments, analyzing research data management plans, and tracking research components, investigator details like names, contact information, affiliated institutions may be stored.

5) Survey Response Information
For survey analysis, participant information like names, emails, phone numbers may be stored.

6) NHLBI Chat user data
For archiving and retrieval purposes, NHLBI Chat collects and stores the user's data including the username, email, and user's NIH ID. Additionally, hiring and/or contracting documentation may include data like license number, photographic identifiers, passport number, and other information related to employment/contracting purposes.

Technical Details:
NHLBI Chat uses an NIH Science and Technology Research Infrastructure for Discovery, Experimentation, and Sustainability (STRIDES) cloud account, which deploys Azure OpenAI models in a secured cloud account. These AI models are static and accessed via an API call. We do not use any data entered into the system to train, fine tune, or deploy new models.

Usage Disclaimer
NHLBI Chat's Landing page requires the user to read through and accept HHS and NIH AI Ethical Use policies as well as the following statement regarding PII usage: "Entering a SSN, EIN or Taxpayer Identification (TIN) is not allowed. Please ensure any PII entered does not include SSN/EIN/TIN. Please ensure any PII entered into NHLBI Chat is deemed absolutely necessary and to the best of your knowledge, permission to use this PII has been obtained separately from the impacted person(s)."

Deleti

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
Driver's License Number
Biometric Identifiers
Mother's Maiden Name
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number

Medical Notes
Financial Accounts Info
Certificates
Legal Documents
Education Records
Device Identifiers
Military Status
Employment Status
Foreign Activities
Passport Number
NIH Identification (ID)
Username
Race, Religion, Age, Sex, Birth Location
Vendor Names, Affiliated Institutions
Employment/Contracting Information

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

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The system uses NIH Login/IAM services to retrieve NIH Login credentials (username and Password) for authentication purposes. NHLBI Chat maintains the NIH ID, user name, and user email in order to ensure the ongoing establishment of use and viewing rights in the system.

Primary purposes PII (excluding SSN/EIN/TIN) may be used for, but not limited to, include:
1) Patient Medical Information
If patients' medical histories are entered for analysis or review, this may include details like names, mother's maiden name, contact information (e.g., email address and phone number) , birth dates, medical record numbers, health conditions, medical notes, financial account information, race, religion, sex, birth locations, photographic and biometric identifiers

2) Staff/Contractor Administrative Information
For drafting documents related to staff renewals, performance evaluations, travel forms, hiring memos, contract staff on-boarding and clearance, details may be included such as: names, contact information (e.g., email address and phone number) , certificates, education records, foreign activities, employment status, legal documents, device identifiers, passport number, age, sex, military status.

3) Vendor Information
If entering vendor information for procurement and purchasing purposes, data like vendor names, emails, phone numbers, mailing addresses, certificates, driver's license numbers, vehicle identifiers, financial account information may be stored.

4) Grant Research Information
When assigning grants to departments, analyzing research data management plans, and tracking research components, investigator details like names, contact information, affiliated institutions may be stored.

5) Survey Response Information
For survey analysis, participant information like names, emails, phone numbers may be stored.

6) NHLBI Chat user data
For archiving and retrieval purposes, NHLBI Chat collects and stores the user's data including the username, email, and user's NIH ID. Additionally, hiring and/or contracting documentation may include data like license number, photographic identifiers, passport number, and other information related to employment/contracting purposes.

Describe the secondary uses for which the PII will be used.
There are no secondary uses.

Identify legal authorities governing information use and disclosure specific to the system and program.
5 U.S.C. 301 and 302, 44 U.S.C. 3101
and 3102.

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.
09-25-0036, Extramural Awards and Chartered Advisory Committees (IMPAC 2), Contract
09-25-0099, Clinical Research: Patient Medical Records; 09-25-0156, Records of Participants in
09-25-0216, Administration: NIH Electronic Directory, HHS/NIH; 09-25-0217, NIH Business System;

Identify the sources of PII in the system.
Directly from an individual about whom the information pertains
Online
Government Sources
Within the OD

Identify the OMB information collection approval number and expiration date
An OMB collection number is not required for this system, as it uses federal employee PII solely for internal purposes. Any additional PII is obtained from source systems, which are responsible for securing the appropriate OMB collection approval number.

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.
a. For PII of NHLBI Chat Users:
There is a disclaimer displayed to users prior to login and remains persistent on the main screen informing them they are accessing a U.S. Government information system and there is “no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the government may monitor, intercept, record, and search and seize any communication or data transiting or stored on this information system. Any communication or data transiting or stored on this information system

may be disclosed or used for any lawful Government purpose."

b. For PII entered as part of a use case defined above:
NHLBI does not directly collect PII information from the public, such as citizens, patients, business partners, vendors, or contractors. However, NHLBI Chat users may enter such information as part of their day to day responsibilities. In these cases, the responsibility to provide notice rests with the original source of the PII, i.e., the organization/system where it was first collected and/or the user. NHLBI has placed terms and conditions the user needs to agree to before the using the tool and contains this guideline:
"Entering SSN, EIN or other Taxpayer ID is not allowed. Please ensure any PII entered does not include SSN/EIN/TIN. If PII (other than SSN/EIN/TIN) is entered, please ensure it is deemed absolutely necessary, and to the best of your knowledge, permission to use this PII has been obtained separately from the impacted person(s). PII is permitted for use and is not limited to genomic data, passport information, driver's license numbers, military status, bank account information including credit card numbers, photographic identifiers, medical record numbers, certificate, education records and date of birth. By entering in PII you accept that incidental storage of the PII as part of the chat record will occur."

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.

There is no opt-out method for users since their email address and log-in credentials are needed for authentication purposes. Individuals do have the option to not submit an email and log-in credentials however, they will not have access to the system.
a. Users of NHLBI Chat (limited to NHLBI internal users) are provided with a landing page, when they launch NHLBI Chat that provides a description of the system, Office of the Chief Information Officer (OCIO) guidance and policy for restriction of public AI tools, as well as guidelines for use of each of the following: Human oversight, limitations and biases, ethical use, use of PII, and training data. The landing page ends with a disclaimer stating the user is accessing a U.S. Government Information system and a user consent/agreement statement. If the user does not agree, then the user does not select to proceed.

b. PII (excluding SSN/EIN/TIN) may be entered into NHLBI Chat as part of the use cases defined above. The system does not directly collect PII; however, system users may enter personal information about individuals based on data previously collected through NIH-authorized channels, i. e., through employment agreements, research contracts,and grant agreements. Since NHLBI Chat is not the original point of data collection, it does not provide a mechanism for non-user individuals to opt out of the use of their information. Users are reminded, as part of the disclaimer, that they are responsible for ensuring that appropriate notice and, where applicable, permission to use such personal information has been obtained prior to entry into the system.

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

The process followed for updating users of changes to the NHLBI Chat includes the following:

1) Notification sent out in the NHLBI Chat teams channel
2) update by email (if warranted)
3) Update of the NHLBI Chat landing page.
4) For Individuals whose PII may be used/present - “NHLBI Chat is not a source system. It does not collect personal information directly from individuals. Instead, it may contain PII that was previously

collected through other authorized systems or organizational processes. Operators of the original source systems are responsible for providing a process to notify individuals and, where applicable, obtain their consent prior to the collection and use of their information and when a major change occurs to the system.

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.

a. If a user has a concern with NHLBI Chat, they are able to use a link to "Submit Feedback" on the NHLBI Chat landing page along with an option to connect via Teams.
b. Additionally, on the NHLBI Intranet page describing NHLBI Chat, users are provided with a link to join the NHLBI Chat Microsoft Teams community, as well as a feedback option to send back comments/questions to the content owner.
c. The Landing page allows users to contact the NHLBI Scientific Information Office via email (nhlbi_dir_sio@nhlbi.nih.gov), phone (301.480.5446), or in-person.
d. The landing page also directs individuals who believe their PII has been inappropriately obtained, used, disclosed, or that it is inaccurate to contact NHLBI Privacy Coordinator Office via email at: NHLBI_PrivacyOffice@mail.nih.gov.

Since NHLBI Chat is not a source system, i.e., it does not collect personal information directly from individuals, it may contain PII that was previously collected through other authorized systems or organizational processes. Operators of the original source systems are responsible for providing a process to notify individuals and, where applicable, obtain their consent prior to the collection and use of their information and when a major change occurs to the system. The operators of the original source are also responsible for providing a resolution process to individuals who believe their PII has been inappropriately obtained.

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 four processes in place:
1) Integrity
The system's annual security assessment includes a review of selected privacy and security control. These reviews help ensure that PII has not been improperly altered and continues to be protected from unauthorized modification. IN addition, user access reviews help maintain data integrity by limiting access to authorized personnel only.
2) Availability
Annual access reviews are conducted to ensure that only current authorized users retain access to the system. This supports availability by ensuring that PII remains accessible to those who need it to perform their job functions while minimizing unnecessary or outdated access.
3) Accuracy
With each system release or functionality change, documentation is reviewed to confirm whether the types of PII collected or used to have changed. This review process helps ensure that PII maintained remains accurate and aligned with the current use and purpose of the system's
4) Relevancy.
The system implements a two-step deletion process for chat data. After 90 days chat content is no longer visible to users. After another 90 days (180 days total), the data is permanently deleted from the database. This process helps ensure outdated or unused PII is not retained longer than necessary, maintaining the relevancy of information held within the system.

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 to PII is granted based on role-based access controls and a policy of least privilege. Users must login to verify identities and privileges, with access provisioned only according to job responsibilities and specific need. System administrators configure permissions and user roles to appropriately restrict data, segregating PII to authorized personnel requiting access. Account access requests undergo review to ensure conformance with access control policies. These controls limit PII access to employees and contractors with need to know.

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 restricted based on role-based access controls and a policy of least privilege. System administrators configure precise permissions and user roles, allowing access to only the minimum amount of PII required for employees and contractors to perform their specific job responsibilities. Users must login to verify identities and privileges, with access strictly provisioned according to defined needs. Requests for account access undergo review to ensure conformance with the access control policy of providing only the minimum necessary PII. These methods segregate data to authorized personnel, limiting PII access to those with a need to know.

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).

Users are provided a "How To" training video on proper chat system usage on the NHLBI Chat landing page and NHLBI Intranet.

In addition, there is a vulnerability disclosure link provided at the chat login screen that allows users to privately and securely report any discovered vulnerabilities.

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.

Chat records are maintained within the system accordingly to the following:
a) Soft-delete after 90 days. Unused chats will disappears from a user’s list.
b) Hard-delete after 90 more days (180 total). The chat will be fully deleted from the database.

This action flags the chat in the server database for administrator to permanently remove according to NHLBI record retention policies and in accordance to
Item 10-004 - Intermediary Records.

Description: Records of an intermediary nature, meaning that they are created or used in the process of creating a subsequent record.
Disposition Instruction: Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Disposition Authority: DAA-GRS-2017-0003-0002

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

Physical Controls: The information technology (IT) hardware used to host protected information is located in a secured datacenter 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.

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. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.