US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/02/2026

OPDIV:

NIH

Name:

NIH OD ChIRP Chat - Intramural

PIA Unique Identifier:

P-1336157-563047

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?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

NIH Office of the Director (OD) ChIRP Chat -Intramural (CCBAI -Intramural) is a client-side, web browser-based user interface Artificial Intelligence (AI) system served from a web server. It is designed to provide users with general information through Large Language Models (LLM) in the Azure Federal Risk and Authorization Management Program (FedRAMP) environment. CCBAI - Intramural is a chat front-end interface designed to provide staff with a secured, chat-like experience for their day-to-day work, through Microsoft Azure's FedRAMP AI Chat services. CCBAI - Intramural provides relevant information based on the user’s conversation with the chat bot. The information is whatever the chat bot determines is relevant and helpful to the end user based on the conversations and inputted questions/requests.

The system operates with user-initiated requests (chats/messages) that are conveyed to the LLM, via an encrypted application programming interface (API). Replies are then conveyed back to the user to form a continuous chat experience. All exchanges are tracked in a database hosted on the server. CCBAI - Intramural is hosted on a Azure Ubuntu Virtual Machine (VM) in the National

Institutes of Health (NIH)/Office of the Director (OD)/Office of Intramural Research (OIR)/ Clinical Research Informatics Strategic Planning Initiative (CRISPI)-LLM-Azure. The system is deployed under STRIDES General Support System (GSS), using Transport Layer Security (TLS) 1.2 secure communication transmission, and is scanned regularly by NIH Tenable Agents and Azure Defender for Cloud.

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.

CCBAI - Intramural collects and stores text information inputted by the user. The system does not require users to submit specific categories of PII for general functionality; however, certain categories of PII are explicitly prohibited and restricted from entry. Users review the rules that apply to them and work with designated Subject Matter Experts to confirm there are no legal or procedural restrictions associated with their use cases. For grant sensitive data use case scenarios, users reach out to NIH Office of Policy for Extramural Research Administration for confirmation that the tool is allowed. Users are alerted that they should have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system.

CCBAI - Intramural collects the following personally identifiable information (PII) Name, Mother's maiden name, email, phone numbers, medical notes, date of birth, mailing address, medical record numbers, device identifiers, employment status, and Photographic and Biometric Identifiers.

Users log in to this system via the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own 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.

NIH Office of theDirector (OD) ChIRP Chat -Intramural (CCBAI -Intramural) is a client-side, web browser-based user interface Artificial Intelligence (AI) system served from a web server. It is designed to provide users with general information through Large Language Models (LLM) in the Azure Federal Risk and Authorization Management Program (FedRAMP) environment. CCBAI - Intramural is a chat front-end interface designed to provide staff with a secured, chat-like experience for their day-to-day work, through Microsoft Azure's FedRAMP AI Chat services. CCBAI - Intramural provides relevant information based on the user’s conversation with the chat bot. The information is whatever the chat bot determines is relevant and helpful to the end user based on the conversations and inputted questions/requests.

The system operates with user-initiated requests (chats/messages) that are conveyed to the LLM, via an encrypted application programming interface (API). Replies are then conveyed back to the user to form a continuous chat experience. All exchanges are tracked in a database hosted on the server. CCBAI - Intramural is hosted on a Azure Ubuntu Virtual Machine (VM) in the National Institutes of Health (NIH)/Office of the Director (OD)/Office of Intramural Research (OIR)/ Clinical Research Informatics Strategic Planning Initiative (CRISPI)-LLM-Azure. The system is deployed under STRIDES General Support System (GSS), using Transport Layer Security (TLS) 1.2 secure communication transmission, and is scanned regularly by NIH Tenable Agents and Azure Defender for Cloud.

The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that

introduce new privacy risks.

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
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Device Identifiers
Employment Status

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

Employees
Public Citizens
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

The primary purpose of the PII will be to help NIH staff perform job duties, including but not limited to analysis of data, streamlining and automation of processes, summarization of information, and to perform predictive analytics.

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

NA

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

5 U.S. Code §301 and 302
42 U.S. Code § 241
42 U.S. Code § 282
42 U.S. Code § 284

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Government Sources
Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A. This system is exempt from an OMB Information Collection Number through Public Law

114-255 - 21st Century Cures Act, Section 2035: Exemption for the National Institutes of Health from the Paperwork Reduction Act 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.

CCBAI - Intramural is not a source system. PII is not collected directly from individuals. Source system operators are responsible for notifying individuals about the uses of their personal information and is covered in the respective source system PIA.

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.

CCBAI - Intramural is not a source system. Personal information is not collected directly from individuals. Source system operators are responsible for providing a method to opt-out of the collection and use of their PII.

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

CCBAI - Intramural is not a source system. Personal information is not collected directly from individuals. Source system operators are responsible for providing a process to notify and obtain consent from individuals whose PII is in the system 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.

CCBAI - Intramural is not a source system. Personal information is not collected directly from individuals. Source system operators are responsible for putting a process in place to resolve an individual's concerns about the collection and use their PII. However, individuals may contact any IC Privacy office, or the NIH Senior Official for Privacy.

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

NIH has implemented the following controls:
PII Detection software
Multi-factor authentication (MLP)

CCBAI - Intramural is not a source system and does not have process in place to review PII. Personal information is not collected directly from individuals. Source system operators are responsible periodically reviewing PII contained in the source systems to ensure data integrity, availability, accuracy, and relevance.

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.

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.

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 and privacy awareness training. Training is completed on the http: //irtsectraining.nih.gov site with valid NIH credentials. Individuals with elevated privileges, such as Administrators, are additionally required to take Role-Based Training Courses.

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

Training and Support is provided within the system on how to use the system, AI guidance and AI risks.

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.

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. Destroy 7 years after cutoff (DAA-0443-2012-0007-0003).

01-005, Institutional Review Board (IRB) Records. Cut off research-specific IRB records annually at the completion of the research project and IRB operational and governance records at the end of each fiscal year or cut off when no longer needed for business and scientific use, whichever is longer. Destroy 3 years after cutoff (DAA-0443-2012-0007-0005).

03-001, Clinical Care Services Records. Cut off annually at end of fiscal year. Destroy 7 years after cutoff (DAA-0443-2019-0001-0001).

03-005, Patient Medical Records. Cut off patient case file annually after 5 years of inactivity. Destroy when case file
is no longer needed for scientific reference (DAA-0443-2012-0007-0010).

03-008, Clinical Care Administrative Support Records. Destroy when 3 years old, but longer retention is authorized if needed for business use (DAA-0443-2018-0002-0001).

Additional records retention schedules may apply depending on the use case and function of the system's data and output(s). Users work with their records liaisons to determine the appropriate records retention schedule and disposition authority.

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

Administrative Controls: Management oversight of activities, security awareness and training for users of the system, conduct disaster recovery exercises, separation of duties for personnel administering the system, isolating development test instances of the system. Additionally, users must select their role at NIH (administrative, research, etc.).

Technical Controls: ChIRP uses the PII Detection tool to remove sensitive data that is not allowed in ChIRP. Additionally, ChIRP uses Security Information and Event Management technology to provide real-time analytics and security alerts to manage security incidents. ChIRP uses NIH IAM for authentication and authorization for all users.

Physical Controls: The system is cloud-based and inherits physical security controls. The system is hosted within the Federal Risk and Authorization Management Program (FedRAMP) approved Microsoft Azure Public Cloud and meets the physical security controls detailed in the FedRAMP Security Assessment Framework.