US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/26/2025

OPDIV:

NIH

Name:

FNLCR CSPSS

PIA Unique Identifier:

P-1066389-078631

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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.

The PIA has been updated to meet the requirements of Executive Order - Defending Women From Gender Ideology Extremism And Restoring Biological Truth To The Federal Government.

Describe the purpose of the system.

This system supports the Frederick National Laboratory for Cancer Research Clinical Services Program Support Services to the National Institute of Allergy and Infectious Diseases (NIAID) (FNLCR CSPSS NIAID), which operates under the FNLCR Applied and Developmental Research Directorate and provides expertise covering a broad spectrum of pre-clinical, clinical trial support, and immunologic testing. Program support can begin at the early stages of clinical trial development to aid in developing a comprehensive strategy for sample collection, processing, and testing with a special emphasis on immunologic testing in patients with cancer, Acquired Immunodeficiency Syndrome (AIDS), other infectious diseases, chronic granulomatous disease, and other diseases associated with immune deficiency and autoimmunity. Program laboratories collaborate with

partners to develop customized assays or transfer existing assay technology with assay validation, data analysis and interpretation of results. FNLCR CSPSS NIAID laboratories also perform high complexity testing under the auspices of the Clinical Laboratory Improvement Amendments, with test results used to aid in patient diagnosis or treatment decisions.

This system includes 21 individual applications that support multiple NIAID studies, as well as the following labs:
Acquired Immunodeficiency Syndrome (AIDS) Monitoring Laboratory (AML)
Laboratory of Molecular Cell Biology (LMCB)
Immunological Monitoring Laboratory (IML)
Neutrophil Monitoring Laboratory (NML)

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

The system collects/stores the following personally identifiable information (PII): study participant name (First and Last), NIH medical record number, medical notes, sex, date of birth, and for some applications, application-specific user credentials. PII is shared with another NIAID system, Clinical Research Information Management System of NIAID (CRIMSON), which has its own approved privacy impact assessment (PIA).

The system also collects/stores the following non-PII: study ID, sample ID, sample type, sample location, and virus genotype sequences. Non-PII related to sample management is manually shared with the Biological Specimen Inventory (BSI). Human Immunodeficiency Virus (HIV) genotype sequences are sent to the Stanford HIV Drug Resistance Database Sierra web service for HIV drug resistance assessment and non-PII is returned regarding any drug resistant sites found in the sequence.

The AML Flow Labels, AML 6 Color Flow Program (AML6Lyric), AML 8 Color Flow Program (AML8Lyric), LMCB Neot Program, LMCB Zetat Program, and NML Assay Request Tracking System (Web interface), do not require authentication. Access is controlled by NTFS (new technology file system – that is, Windows file permissions).

Users authenticate (log in) to the following applications with an application-specific user identifier (ID) and password, or just a password: AML Patient System, AML NIAID Patient Sample Database (DB) System (Update/Reports & View Modules), AML Yarchoan Patient Sample DB System, AML Flow Differential Entry (AMLDIFF) System, IML Sample Tracking System, NIAID PREPARE (Ebola-Zaire Vaccine Protocol).

Users for AML Repository Viewing System, NML Sample Tracking System, NML Assay Request Tracking System (Windows interface), NIAID INARC (COVID-19 Protocol), and NIAID INVITE (COVID-19 Protocol) use authentication services (log in) provided by the NIH Identity, Credential, and Access Management (IAM) Services, which maintains its own unique PIA on record, including all legal authorities documented. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service that facilitates and governs network access to various resources. These applications only use Windows authentication via LDAP (lightweight directory access protocol), and do not use multi-factor authentication with an NIH personal identity verification (PIV) card.

The following applications currently use an application specific user ID and password but are in the final testing stage of being converted to use NIH IAM Services: NIAID H1Flu (H1N1 FLU Protocol), NIAID FIVFlu (FLU-IVIG (intravenous immunoglobulin) Protocol), NIAID SILCAAT (subcutaneous, recombinant, human interleukin-2 in HIV-infected patients with low CD4+ counts under active antiretroviral therapy) Human Immunodeficiency Virus (HIV) Protocol), NIAID IRCX (IRC003 & IRC004 Influenza Protocols), and NIAID ESPRIT (evaluation of subcutaneous proleukin in a

randomized international trial) Protocol).

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

This system supports the FNLCR CSPSS NIAID, which operates under the FNLCR Applied and Developmental Research Directorate and provides expertise covering a broad spectrum of pre-clinical, clinical trial support, and immunologic testing. Program support can begin at the early stages of clinical trial development to aid in developing a comprehensive strategy for sample collection, processing, and testing with a special emphasis on immunologic testing in patients with cancer, AIDS, other infectious diseases, chronic granulomatous disease, and other diseases associated with immune deficiency and autoimmunity. Program laboratories collaborate with partners to develop customized assays or transfer existing assay technology with assay validation, data analysis and interpretation of results. FNLCR CSPSS NIAID laboratories also perform high complexity testing under the auspices of the Clinical Laboratory Improvement Amendments, with test results used to aid in patient diagnosis or treatment decisions.

This system includes 21 individual applications that support multiple NIAID studies, as well as the following labs: AML, LMCB, IML, NML.

The system collects/stores the following PII: study participant name (First and Last), NIH medical record number, medical notes, sex, date of birth, and for some applications, application-specific user credentials. PII is shared with another NIAID system, CRIMSON, which has its own approved PIA.

The system also collects/stores the following non-PII: study ID, sample ID, sample type, sample location, and virus genotype sequences. Non-PII related to sample management is manually shared with the BSI. HIV genotype sequences are sent to the Stanford HIV Drug Resistance Database Sierra web service for HIV drug resistance assessment and non-PII is returned regarding any drug resistant sites found in the sequence.

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
Medical Records Number
Medical Notes
sex
User Credentials - application-specific (usernames and passwords)

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?

10,000-49,999

For what primary purpose is the PII used?

PII is used for research and clinical reporting purposes.

HHS user credentials are used to control access to some applications. Application-specific user credentials are used to control access to some applications.

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

PII can be used by developers when testing FNLCR CSPSS NIAID applications to ensure the data has been written accurately.

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

45 CFR 46; 42 USC 241; 42 USC 282; 42 USC 284; 42 USC 285f

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 & Population-based Research Studies of the NIH

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

Email

Online

Government Sources

Within OpDiv

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

Not Applicable. Public Law 114-255, Section 2035, exempts research conducted by NIH from 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.

Study participants provide/document their consent with an NIH Institutional Review Board (IRB)-approved consent form. The consent form states that medical information will be stored in NIH medical information systems.

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.

Participation in clinical studies is voluntary; however, PII is required for clinical research/participation. Should a participant opt-out of providing the required PII, the participant is in effect opting out of the entire study.

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

When an initiative arises in which historical data or specimens are desired for use in ways not covered by prior consent, the IRB reviews and advises on the scope of consent. In many cases the IRB requires re-consent with the study participant or requires that program refrain from data or specimen uses not previously consented.

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.

The process to resolve individual's concerns about their PII and how it is being used is done through the Principal Investigator (PI) leading each case study and the NIH IRB. Participants can reach out to their respective PI via email or phone; and work with them to correct any issues.

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

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy. The system produces reports for review by laboratory personnel who reviews the assay data results for accuracy and system administrators who reviews for discrepancies and report back to the study coordinators.

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.

Users authenticate (log in) to some applications with an application-specific user ID and password or just a password; only users with valid accounts are granted access to those applications. Some applications rely on user authentication services provided by the NIH IAM Services; only users with valid NIH accounts are granted access to those applications.

Administrators have access to all PII in the system. Access to PII within an application is assigned to personnel based upon current job responsibilities. Study participants whose data is in the system do not have access to any of the applications.

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.

Application-specific credentials are required to access the stored PII data in some applications. User authentication services for some applications are provided by the NIH IAM Services; only users with valid NIH accounts are granted access to those applications.

Administrators have access to all PII in the system. Access to PII is assigned to personnel based upon current job responsibilities. Study participants whose data is in the system do not have access to any of the applications.

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 security awareness training. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management, and Emergency Preparedness). 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).

Additional training is required for individuals with significant security responsibilities. In addition, users are required to take annual Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) 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.

Study participant records pertaining to FNLCR CSPSS NIAID are retained and disposed of under the authority of the following NIH Records Schedule:
Item 01-003: Records of All Other Intramural Research Projects.
These records do not meet the retention criteria for Item I-0001 - Records of Intramural Research Records Projects of Historical Significance, or Item I-0002 - Research Records that Support Intellectual Property Rights.
Disposition: 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

Login /Systems Access Records are retained and disposed of under the authority of the following NIH Records Schedule:
Item 07-203: System Access Records. Systems not requiring special accountability for access. System Access Records. 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 not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users.
Disposition: Destroy when business use ceases. 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: The system had a security assessment and authorization (SA&A) performed in accordance with NIH and HHS requirements. SA&A documentation including the following were developed as required: security categorization, e-authentication risk assessment, system security plan, evidence of security control testing, and plan of action and milestones. Applicable Privacy Act clauses are inserted in solicitations and contracts as applicable. Policies for the retention and destruction of PII are in place. The Clinical Services Program (CSP) Data Management Group (DMG) performs backups of system data on a regular basis.

Technical Controls: Access to some applications does not require authentication, rather is controlled by NTFS (new technology file system – that is, Windows file permissions). Users authenticate (log in) to some applications with an application-specific user ID and password or just a password. Some applications rely on user authentication services provided by the NIH IAM Services. Logical access controls restrict access to the servers hosting the system to only those administrators requiring access to maintain the servers and the applications. Data travels over secured NIH networks. Intrusion detection is provided by the NIH network at the perimeter and other points within the network. The NIH Incident Response Team is responsible for incident handling, response, and reporting, and will notify the NIAID Information Systems Security Officer of any incidents that can be related to the system. FNLCR CSPSS NIAID is not publicly accessible and can only be accessed from within the NIH network.

Physical Controls: System components are located in NIH data centers, which have appropriate physical controls to restrict access to servers. Access to data centers is controlled by NIH PIV card. Visitors are always escorted.