US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/14/2024

OPDIV:

NIH

Name:

DTM Stemlab

PIA Unique Identifier:

P-3416611-285817

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?

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.

This validation is intended to refresh content and update the security authorization date. There have been no substantial changes since the last assessment.

Describe the purpose of the system.

StemLab is a clinical and administrative management system that helps the NIH Clinical Center (CC) Cell Processing Section (CPS) with operational and manufacturing details, while assisting CPS staff with accreditation compliance, ensuring processing standardization and increasing access to CPS StemLab data.

StemLab also supports stem cell processing operations for bone marrow and apheresis (the removal of blood plasma from the body by the withdrawal of blood, its separation into plasma and cells, and the reintroduction of the cells, used especially to remove antibodies in treating autoimmune

diseases) products.

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

Donor and NIH research participant information related to stem cell processing operations include. Name, Phone Numbers, Medical Notes, Date of Birth (DOB), Mailing Address, Medical Records Number (MRN), Device Identifiers, referring physician name and address, visit number, medication order number, and laboratory results. Donations must be directly attributable to each individual donor.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 collects unique user credentials and stores them in an encrypted format. The IAM Service is 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.

StemLab is a clinical and administrative management system that helps the CPS with operational and manufacturing details while assisting other CPS staff with accreditation compliance, ensuring processing standardization and increasing access to CPS StemLab data. StemLab also supports stem cell processing operations for bone marrow and apheresis products.

Donor and National Institutes of Health (NIH) research participant information related to stem cell processing operations includes Name, Phone Numbers, Medical Notes, DOB, Mailing Address, MRN, Device Identifiers, referring physician name and address, visit number, medication order number, and laboratory results. Donations must be directly attributable to each individual donor.

Those requiring access to this system log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

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
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Device Identifiers
Referring physician name and address
Visit number, medication order number and laboratory results

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

Employees
Public Citizens
Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Information related to donation and receipt of blood products for patients on Institutional Review Board (IRB) approved protocols is shared with intramural clinical research team.

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

There have been no secondary uses specified by the system owner.

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

The legal authority to operate and maintain this Privacy Act records system is 42 U.S.C. §§ 241, 248, 282 and 284

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.

09-25-0011, Clinical Research: Blood Donor Records, HHS/NIH/CC

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

In-Person

Online

Government Sources

Within OpDiv

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

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.

Individuals are notified that their personal information will be collected when they present for donation at the Clinical Center (CC) for blood donation. Each individual is provided a formal notification of Information Practices and must certify that they have been so advised.

Every patient must voluntarily execute a protocol consent and authorization prior to entry onto an intramural research protocol and treatment at the Clinical Center. In addition, each patient is provided a formal notification of Information Practices at the Clinical Center and must certify that they have been so advised.

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.

General admission and protocol consent forms are signed by each patient. Additionally, an

information practices notification form is reviewed and acknowledged in writing by each patient at the time of initial admission to the CC. Enrollment in a clinical research trial is voluntary and the collection of Personally Identifiable Information (PII) and medical notes is necessary to conduct research and provide clinical care. Therefore, a patient may not opt out of the collection or use of their PII while participating in research at the CC.

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

General admission and protocol consent forms are signed by each patient. Additionally, an information practices notification form is reviewed and acknowledged in writing by each patient at the time of initial admission to the CC. Enrollment in a clinical research trial is voluntary and the collection of PII and medical notes is necessary to conduct research and provide clinical care. Therefore, a patient may not opt out of the collection or use of their PII while participating in research at the CC.

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 Privacy Rights Complaint Form is available to individuals when they believe that their PII has been inappropriately used or disclosed. The Clinical Center's Privacy Office will review the complaint and respond to the concern within 30 business days. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC Privacy Officer.

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

Modifications to patient PII such as name, MRN, visit number or medication order number are sent from Clinical Research Information System (CRIS) to the system to keep the patient PII in synch across the ancillary clinical information systems. CRIS maintains its own PIA, including all legal authorities documented.

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 assigned to personnel based upon current job responsibilities. A standard NIH IAM Services account is required to gain access to the stored PII data. (The availability of PII data is based on file system permissions and the access rights of the logged-on user's NIH IAM Services account determines whether PII may be accessed).

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.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles. Authentication with NIH Personal Identity Verification (PIV) card will occur at time of login to the NIH Network. System owners are responsible for creating the proper security groups within their systems with the applicable permissions for group members to enforce least privilege.

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. 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.

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

Application specific peer training is available based on role and permissions.

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 Intramural Records Retention Schedule.

Item 03-005: Patient Medical Records.
These records document admissions and medical treatment for a patient accepted in a research project.
Disposition: 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

Item 03-003 - Blood Donor and Receiving Records
These records relate to blood and its components that are collected, processed, compatibility tested, stored, and distributed by NIH. These records identify blood donors, document donor deferrals, and identify and describe blood products received from other collection facilities. These records shall be retained for such intervals beyond the expiration date for the blood or blood component as necessary to facilitate the reporting of any unfavorable clinical reactions as required by 21 CFR 606.
Disposition: Cut off annually after 50 years or annually after expiration of the patient/subject, whichever is longer. Transfer to inactive storage 1 year after cutoff. Destroy 30 years after cutoff. DAA-0443-2012-0007-0008

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

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 training and awareness classes and refreshers. Personnel accessing these systems use privileged and separate accounts for administrative access to systems.

Technical Controls: The IT hardware and software used to host information 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.

Physical Controls: The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.