

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

06/30/2025

**OPDIV:**

NIH

**Name:**

CWA: Phlebotomy Wait Time Tracker

**PIA Unique Identifier:**

P-6653577-315796

**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. There have been no substantial changes since the last assessment.

**Describe the purpose of the system.**

The Phlebotomy Wait Time Tracker (WTT) tracks all of the patients that receive a blood draw, known as phlebotomy, and what specific actions were taken.

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

The system stores the following: ticket number, the phlebotomist's initials, and patient's Medical Records Number (MRN) and medical notes (patient time of arrival, time of services, what sterile vacuum sealed blood collection tubes were drawn, type of patient (pediatric or adult), whether a urine sample was provided (yes/no flag)).

Users log in to this system using the NIH Identity, Credential, and Access Management (IAM)

Services which maintains its own unique privacy impact assessment (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.**

The Phlebotomy WTT tracks all phlebotomy patients and what specific actions were taken.

The system stores the following: ticket number, the phlebotomist's initials, and patient's MRN and includes medical notes (patient time of arrival, time of services, what sterile vacuum sealed blood collection tubes were drawn, type of patient (pediatric or adult), whether a urine sample was provided (yes/no flag)).

The system uses specific login information to assign permissions/user roles using the NIH IAM Services which maintains its own unique PIA 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.**

Medical Records Number

Medical Notes

Ticket number, Phlebotomists initials

**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?**

5,000-9,999

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

Documentation of care and the service provided.

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

None.

**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.**

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

Directly from an individual about whom the information pertains

In-Person

Government Sources

**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.**

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, only prior to 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.**

All patients are notified of information practices upon admission. Each patient would be advised at the time of the next admission about major system changes and the CC Information Practices Notice would be revised and provided to each patient again.

**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 CC Department of Clinical Research Informatics (DCRI) Privacy Office will review the complaint and coordinate with the NIH Office of the Senior Official for Privacy (OSOP) to respond to the concern. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC DCRI Privacy Office.

**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 PII are sent from the Clinical Research Information System (CRIS) to keep the PII in synchronization across the ancillary clinical information systems.

**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.

**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. Dual factor authentication with NIH Personal Identity Verification (PIV) card and NIH IAM Services account 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. 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).**

Application specific one-on-one peer training is provided as needed.

**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.

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.**

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 public networks to prevent unauthorized or malicious access. Access to the system is controlled by NIH login which authenticates the user prior to granting 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.