

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

03/11/2025

**OPDIV:**

NIH

**Name:**

CRSS: Admission, Travel and Voucher Request System

**PIA Unique Identifier:**

P-5208652-835941

**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.**

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.**

The NIH Clinical Center (CC) Clinical Research Information System (CRIS) supports the diverse functions required to provide clinical care to CC patients and facilitate the collection of NIH intramural research program (IRP) protocol requirements.

The Admission Travel and Voucher Request System (ATV) is a web-application used to submit requests to admit new patients and update existing patient information in CRIS. ATV is also used to request Government-Arranged Travel/Lodging for patients; and request payment vouchers for transportation, lodging and meals.

The CRIS Cloverleaf Integrator (also known as Quality Data eXchange (QDX) interface engine algorithm creates a unique medical record number (MRN) for new patients and provides the MRN to CRIS where it is picked up by the ATV system. CRIS Cloverleaf Integrator QDX maintains its own unique privacy impact assessment (PIA), with all legal authorities documented.

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

The ATV system collects and stores Patient personally identifiable information (PII) to register an individual as a CC patient, a participant in a clinical trial, make travel/lodging arrangements, and provide reimbursement. The ATV system collects Social Security Number (SSN ) for a subset of patients receiving reimbursement or payment for participation, name, email address, phone number (s), medical notes, sex, MRN, date of birth (DOB), demographics and mailing address.

Patient PII is also used to process travel reimbursement request payments in the NIH Business System (NBS) Finance system and the Patient Travel Module. NBS maintains its own unique privacy impact assessment with all legal authorities documented. Information is shared with Omega Patient Travel agents to assist in making the necessary travel arrangements.

NIH staff PII includes the name and email address of the attending physician and primary provider listed in the patient's record in CRIS. It also collects the name of the staff submitting the ATV request.

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.**

The NIH CC CRIS supports the diverse functions required to provide clinical care to CC patients and facilitate the collection of NIH IRP protocol requirements.

The ATV is a web application used to submit requests to admit new patients and update existing patient information in CRIS. ATV is also used to request Government-Arranged Travel/Lodging for patients; and request payment voucher for transportation, lodging and meals.

The CRIS Cloverleaf Integrator QDX interface engine algorithm creates a unique MRN for new patients and provides the MRN to CRIS where it is picked up by the ATV system. CRIS Cloverleaf Integrator QDX enables the exchange of patient clinical data, including Admission, Discharge and Transfer, orders, results, documents, and appointment data, to be transferred seamlessly between CRIS and specified clinical information subsystems connected to it.

The ATV system collects and stores Patient PII to register an individual as a CC patient, a participant in a clinical trial, make travel/lodging arrangements, and provide reimbursement. The ATV system collects SSN for a subset of patients receiving reimbursement or payment for participation, name, email address, phone number(s), medical notes, Sex, MRN, DOB, demographics and mailing

address.

Patient PII is also used to process travel reimbursement request payments in the NBS Finance system and the Patient Travel Module. NBS maintains its own unique privacy impact assessment with all legal authorities documented. Information is shared with Omega Patient Travel agents to assist in making the necessary travel arrangements.

NIH staff PII includes the name and email address of the attending physician and primary provider listed in the patient's record in CRIS . It also collects the name of the staff submitting the ATV request.

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.

CRIS, CRIS Cloverleaf (QDX) and NIH ICAM Services maintain their own unique PIAs, 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.**

Social Security Number  
Date of Birth  
Name  
E-Mail Address  
Mailing Address  
Phone Numbers  
Medical Records Number  
Medical Notes  
Demographics, Sex

**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?**

100,000-999,999

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

The patient PII is primarily used for patient care and support for research participation.

NIH staff PII is primarily used to identify the attending physician and primary provider listed in the patient's record in CRIS.

**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.**

09-25-0099, Clinical Research: Patient Medical Records

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

Directly from an individual about whom the information pertains

In-Person

Hardcopy

**Identify the OMB information collection approval number and expiration date**

Governmental Sources: 4255, Section 2035, exempts research conducted by NIH from Paperwork

Reduction Act (PRA) requirements.

Non-Governmental Sources

Public

**Is the PII shared with other organizations?**

Yes

**Identify with whom the PII is shared or disclosed and for what purpose.**

**Describe any agreements in place that authorizes the information sharing or disclosure.**

HHS has a contract with Omega Travel to arrange travel for patients. Individual travel authorization requests can be printed or retrieved from the ATV system by staff in the CC Admissions office, Omega Patient Travel office and the CC Patient Voucher office.

**Describe the procedures for accounting for disclosures.**

Information disclosed to Omega Travel is covered under the routine uses published in the System of Record Notice (SORN). Omega Travel keeps records of disclosures made when arranging travel for CC patients.

**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 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.

If a patient does not want to provide their SSN then he/she is not eligible to receive government funds in the form of government-arranged travel or travel reimbursement payments. The patient can still participate in clinical research without providing a SSN.

**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 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.**

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy. The system produces print outs for review by travel agents, CC Admissions office staff, NIH intramural researchers and project administrators. With each admission, the Admissions office staff verbally verify the patient's name, DOB, address, and phone number. Patients have an opportunity to correct any changes since the last visit to the Clinical Center. The patient reimbursement process requires patients to complete a request form with name and address. The request form is compared to patient information in ATV for verification. ATV requestors and patients may submit demographic updates and this ensures the integrity of their PII.

CRIS is the official repository of PII, so ATV monitors patient records in CRIS for updates on a nightly basis. Where a record containing changed demographic information is found, the patient's PII is refreshed from CRIS to keep the systems in synchronization.

**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 based on the user's role. Application administrators assign account permissions based on the user's role and current job responsibilities.

**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.**

An active NIH IAM account is required at login. General users have permissions to access only the PII necessary to perform their assigned role. Administrators have permissions to access all the PII stored in the ATV system. System owners are responsible for creating the proper security groups within their system with the applicable permissions for group members to enforce least privilege. The ATV system owner approves all changes and delegates responsibility for configuration to the ATV system administrator.

**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.

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 training for ATV includes completing online computer-based training (CBT) before an account is created. Administrators will provide one-on-one training if users have questions after completing the CBT.

**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 03-001: Clinical Care Services Records

These records consist of clinical care services and clinical care department operational records that are consolidated under this one common temporary retention item. Exclusions and exceptions are noted and cross referenced to their appropriate item numbers within this schedule.

Disposition: TEMPORARY. Cut off annually at end of fiscal year. Destroy 7 years after cutoff. ( DAA-0443-2019-0001-0001 )

**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.