

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

03/11/2025

**OPDIV:**

NIH

**Name:**

CWA: Bioethics Consult

**PIA Unique Identifier:**

P-3813733-613766

**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.**

To record consultations done by the Bioethics Consultation Service. The system will collect and maintain the reason for the consult, background information relevant to the consult, analysis and recommendations of the consult service, who requested the consult, and details regarding any research participant who is the focus of the consultation.

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

Information related to bioethics consultations between NIH Clinical Center (CC) patients and ethics staff and attending physicians. This information includes name, medical notes, medical records number(s) (MRN), diagnosis, age, sex, family members in attendance, primary ethicist, and attending physician.

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

To record consultations done by the Bioethics Consultation Service. The system will collect and maintain the reason for the consult, background information relevant to the consult, analysis and recommendations of the consult service, who requested the consult, and details regarding any research participant who is the focus of the consultation.

Information related to bioethics consultations between the NIH CC patients and ethics staff and attending physicians. This information includes name, medical notes, MRNs, diagnosis, age, sex, family members in attendance, primary ethicist, and attending physician.

Users log in to this system using the NIH IAM Services which maintains its own unique PIA on record, including 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.**

Name  
Medical Records Number  
Medical Notes  
Attending physician, Family members in attendance  
Primary ethicist, Diagnosis, Age, 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?**

50,000-99,999

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

Record keeping and quality improvement related to bioethics consultations between NIH CC patients and ethics staff and attending physicians.

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

Research related to medical ethics (contributions to studies have Personally Identifiable Information (PII) de-identified).

**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.**

09-25-0200, Clinical, Basic and Pop. based NIH Research Studies

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

Other

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

With Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

Public

**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 CC. In addition, each patient is provided a formal notification of Information Practices at the CC 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.

**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.**

Information, including PII, is reviewed when queries are performed and data is provided to the clinical research team. Modifications to patient PII are sent from Clinical Research Information System (CRIS) to the system to keep the patient PII in synch 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.

**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.

Administrative access is limited to authorized CC staff 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. 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 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?**

No

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

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 03-006: Medical Staff Credentialing Records

Medical Staff credentialing records documenting approval of physicians, dentists, and other health professionals for involvement in patient treatments or other patient contacts. These records document participation in patient care and include signed agreements to abide by Medical Staff bylaws, delineations of clinical privileges, and related records. Information is collected from individual members of the Clinical Center Medical Staff and is used to document their credentialing and privileging.

Disposition: Cut off annually after medical staff member leaves patient care. Transfer to inactive storage 1 year after cutoff. Destroy 30 years after cutoff. DAA-0443-2012-0007-0011

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

Infrastructure supporting the system is located in the CC or Center for Information Technology (CIT) Datacenter that is on a Federal government campus, protected by armed guards, and behind secured doors where all entry and exit is tracked, monitored, and restricted to authorized individuals only (monitoring is 24/7).

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 CIT Datacenter 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.