US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/20/2025

OPDIV:

NIH

Name:

CCITIN: NAS

PIA Unique Identifier:

P-1874839-814275

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

Significant System Management Change

Describe in further detail any changes to the system that have occurred since the last PIA.

This is a refresher to update the authorization date and note that the system has moved from the Clinical Center Information Technology and Network Infrastructure (CC ITNI) General Support System (GSS) to the Clinical Research Support Services GSS.

Describe the purpose of the system.

The NIH Clinical Center (CC) uses three types of primary network mass storage systems: CC Network Attached Storage (NAS) CCFILE, CC Clinical NAS CCRESEARCH and CC Clinical NAS Isilon (or CC0PISILON). These are physical (hardware) devices that are designed and built to store information produced by employees and direct contractors working at the Clinical Center.

CCFILE is the designated storage volume for all files that do not contain patient or personnel PII data. Although PII data is not intended for this file system, it has the highest levels of security

provided by encryption and access controls because there may be some patient or personnel PII on it.

CCRESEARCH is a storage volume for files that contain patient information as well as any information that may be sensitive in nature (such as Human Resources related information, for example) and that requires the highest levels of security provided by encryption and access controls. This system was the precursor to Isilon.

CC CLIN NAS Isilon is the designated storage volume for all files that contain patient information as well as any information that may be sensitive in nature (such as Human Resources (HR) related information) and that requires the highest levels of security provided by encryption and access controls.

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

CCFILE, CCRESEARCH and Isilon are information technology (IT) hardware infrastructure. The data on CCRESEARCH, Isilon, and to a lesser extent CCFILE, is data related to the vast expanse of medical research and the many protocols running at the NIH Clinical Center.

A user consciously saves their file for future reference on one of the NAS storage systems. Files are created using common productivity applications such as Microsoft Word, Excel, or Adobe Acrobat. Files stored may also be application generated, such as a report from a HR system or a clinical system. (These applications/systems maintain their own unique privacy impact assessments (PIAs).)

Saved files can contain Social Security Number (SSN), patient or staff name, mother's maiden name, E-mail address, phone number, medical notes, educational records, military status, foreign activities, taxpayer identification (ID), date of birth (DOB), photographic identifiers, employer information, biometric identifiers, mailing address, Medical Records Numbers (MRN), financial account information, legal documents, NIH Clinical Research Information System (CRIS) order identification (ID), appointment dates, medical research data, resumes, certificates, taxes and/or legal paperwork . By NIH policy, users who leverage these services are not to store sensitive or personally identifiable information (PII) data in them unless that data is accounted for within another security authorization boundary and is separately assessed for privacy and security compliance and has its own PIA, which is routinely reviewed and updated as needed.

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 NIH Clinical Center (CC) uses three types of primary network mass storage systems: CC Network Attached Storage (NAS) CCFILE, CC Clinical NAS CCRESEARCH and CC Clinical NAS Isilon (or CC0PISILON). These are physical (hardware) devices that are designed and built to store information produced by employees and direct contractors working at the Clinical Center. This is a unified privacy impact assessment (PIA) for the three CC network attached storage (NAS) systems (CCFIL, CCRESEARCH and Isilon (or CC0PISILON).

CCFILE is the designated storage volume for all files that do not contain patient or personnel PII data. Although PII data is not intended for this file system, it has the highest levels of security provided by encryption and access controls because there may be some patient or personnel PII on it.

CCRESEARCH is a storage volume for files that contain patient information as well as any information that may be sensitive in nature (such as Human Resources related information, for example) and that requires the highest levels of security provided by encryption and access controls. This system was the precursor to Isilon.

CC CLIN NAS Isilon is the designated storage volume for all files that contain patient information as well as any information that may be sensitive in nature (such as Human Resources (HR) related information) and that requires the highest levels of security provided by encryption and access controls.

CCFILE, CCRESEARCH and Isilon are information technology (IT) hardware infrastructure. The data on CCRESEARCH, Isilon, and to a lesser extent CCFILE, is data related to the vast expanse of medical research and the many protocols running at the NIH Clinical Center.

A user consciously saves their file for future reference on one of the NAS storage systems. Files are created using common productivity applications such as Microsoft Word, Excel, or Adobe Acrobat. Files stored may also be application generated, such as a report from a HR system or a clinical system. (These applications/systems maintain their own unique privacy impact assessments (PIAs).)

Saved files can contain Social Security Number (SSN), patient or staff name, mother's maiden name, E-mail address, phone number, medical notes, educational records, military status, foreign activities, taxpayer identification (ID), date of birth (DOB), photographic identifiers, employer information, biometric identifiers, mailing address, Medical Records Numbers (MRN), financial account information, legal documents, NIH Clinical Research Information System (CRIS) order identification (ID), appointment dates, medical research data, resumes, taxes and/or legal paperwork . By NIH policy, users who leverage these services are not to store sensitive or personally identifiable information (PII) data in them unless that data is accounted for within another security authorization boundary and is separately assessed for privacy and security compliance and has its own PIA, which is routinely reviewed and updated as needed.

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.

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
Photographic Identifiers
Biometric Identifiers

Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Certificates
Legal Documents
Education Records
Military Status
Foreign Activities
Taxpayer ID
CRIS order ID
Appointment dates, medical research data, resumes, taxes, legal paperwork
Employer information

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

The data on CCRESEARCH and Isilon, and to a lesser extent CCFILE, is data related to the vast expanse of medical research and the many protocols running at the NIH Clinical Center.

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

There is no secondary use.

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?

No

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
Other

Identify the OMB information collection approval number and expiration date

Pub L 104-13 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.

Data saved on these file storage systems are from other source systems (commercial applications, NIH enterprise systems). Notification is the responsibility of the source system.

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.

Data saved on these file storage systems are from other source systems (commercial applications, NIH enterprise systems). Notification is the responsibility of the source system.

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

Data saved on these file storage systems are from other source systems (commercial applications, NIH enterprise systems). Consent is the responsibility of the source system.

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.

Data saved on these file storage systems are from other source systems (commercial applications, NIH enterprise systems). Resolution is the responsibility of the source system.

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

Data saved on these file storage systems are from other source systems (commercial applications, NIH enterprise systems). Notification is the responsibility of the source system.

However, the NIH IT Privacy Program requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected 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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

Access to PII is assigned to personnel based upon current job responsibilities. An IAM account login 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.

Determinations are made based on role-based access controls and least privilege. Access to PII is assigned to personnel based upon current job responsibilities. An IAM account login is required to gain access to the stored PII data.

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).

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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 03-001: 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

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: The IT hardware and software used to host the protected 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.

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. Personnel accessing these systems use privileged and separate accounts for administrative access to systems.

Remote access to this system is permitted via NIH virtual private network (VPN) or Clinical Center Citrix. These systems maintain their own unique PIAs.