US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/10/2025

OPDIV:

NIH

Name:

CRSS: Research PACS (Research Picture Archiving and Communication System)

PIA Unique Identifier:

P-6729404-096230

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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 Clinical Center (CC) Clinical Research Support Services (CRSS) Research Picture Archiving and Communication System (ResearchPACS), also known as Synapse Vendor Neutral Archive (VNA) from Fuji Medical Systems, is a picture archiving and communication system that collects and disseminates medical images and associated data for NIH Institutional review Board (IRB) approved human and animal protocols.

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

The ResearchPACS stores Digital Imaging and Communications in Medicine (DICOM) encoded images of patients, animals and phantoms (specialized objects used for quality control and imaging equipment calibration) along with other ancillary information which may contain personally

identifiable information (PII), including names, dates of birth, medical record numbers, medical notes, sex on NIH intramural research subjects for clinical research and analysis, referring Institute and referring physician.

The National Heart, Lunch and Blood Institute (NHLBI) has a multi-site research protocol that include analysis of medical images obtained on study participants from Henry Ford Health System (HFFS) and Emory Medical Center and the CC. These are sent to Research PACS using virtual connections.

Images shared for research or publication outside of NIH are anonymized to protect the patient's identity using functionality in the NIH Biomedical Translational Research Information System (BTRIS). BTRIS maintains its own unique privacy impact assessment (PIA), with all legal authorities documented.

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 ResearchPACS, commercially known as Fuji SynapseVNA, is a picture archiving and communication system that collects and disseminates medical images and associated data for NIH IRB approved human and animal protocols.

The ResearchPACS stores DICOM encoded images of Patients, animals and phantoms along with other ancillary information which may contain PII, including names, dates of birth, medical record numbers, medical notes, or sex on NIH intramural research subjects for clinical research and analysis.

NHLBI has a multi-site research protocol that include analysis of medical images obtained on the study participants from HFFS and Emory Medical Center and the CC. These are sent to Research PACS using virtual connections.
Images shared for research or publication outside of NIH are anonymized to protect the patient's identity using functionality in the NIH BTRIS.

Those requiring access to this system log in using the NIH IAM Services. NIH IAM Services and BTRIS 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.

Date of Birth
Name
Medical Records Number
Medical Notes
Sex, research subject's DICOM images
Institute sending images, ordering physician's last name

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?

PII is used to identify patients.

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

PII is used for research.

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 Population-Based NIH Research

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Government Sources
Within the DOI

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?

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.

A Memorandum of Understanding (MOU) exists between the NIH Clinical Center (CC) and Henry Ford Health System (HFHS) for passing one-way data between a PACS system located at HFHS and the Clinical Center's Research PACS located at the NIH via the Federal Information Processing Standards (FIPS) 140-2 approved Virtual Private Network (VPN).

A Memorandum of Understanding (MOU) exists between CC and Emory University for passing one-way data between a PACS system located at Emory Medical Center and the Clinical Center's ResearchPACS at the NIH via the Federal Information Processing Standards (FIPS) 140-2 approved VPN.

Specifically, HFHS and Emory Medical Center will pass data to NIH's Research PACS for use by NHLBI.

Describe the procedures for accounting for disclosures.

Procedures for accounting:
1. If a request for an accounting is received, there are audit logs to allow the system owner to provide that information.
2. Accounting for disclosures requires both automated and manual processes to compile in systems containing PII. Disclosure to others by the party accessing that information is a manual process, and this may be a formal manual process (tracked with a spreadsheet, for example) or an ad-hoc process (tracked after the fact, only upon request, using information such as notes or emails).

The system owner will work with the application administrator to review audit logs to identify persons accessing the requesting individual's information. Tracking the recipient and purpose of PII disclosures to an outside party is a manual process and varies for each instance.

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. Major changes in the use of their DICOM images in the ResearchPACS would be incorporated in an amended CC Information Practices Notice and provided to the CC patients at the time of next admission.

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.

Log files are reviewed daily by system managers to ensure the data's integrity, availability, accuracy and relevancy. System reports are generated daily listing exams transmitted into the system and exams retrieved from the system - this includes origin and destination.

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. The availability of PII data is based on file system permissions and the access rights of the user's 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.

Access to PII is assigned to personnel based upon current job responsibilities.

A NIH INIH AM Systems 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 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 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 Intramural Retention Schedule.

Item 07-204 - System access records. Systems requiring special accountability for access.
These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Disposition: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. DAA-GRS-2013-0006-0004.

Item 03-022 - Radiology and Imaging Records

These records are comprised of X-rays and other roentgenographic images produced by devices and procedures, such as bodyhead scans created by computerized transaxial tomography (CT). Files may include physician interpretations of images/scans.
Disposition: Cut off in 5 year intervals by fiscal year after file becomes inactive or when no longer needed for clinical reference, whichever is longer. Destroy 60 years after cutoff.
(DAA-0443-2012-0007-0007)

07-201 - Systems and data security records
These are records related to maintaining the security of information technology (IT) systems and data.
Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific
systems for which they were written. This series also includes analysis of security policies, processes, and
guidelines, as well as system risk management and vulnerability analyses.
Disposition: Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.
DAA-GRS-2013-0006-0001

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.