US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/20/2025

OPDIV:

NIH

Name:

Frederick Physical Access Control System

PIA Unique Identifier:

P-2197614-152711

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.

Contractor

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.

N/A

Describe the purpose of the system.

The primary purpose of the National Institutes of Health (NIH) Frederick Physical Access Control System (PACS) is to manage physical access to National Cancer Institute - Frederick (NCIF) facilities, access through perimeter gates at the Advanced Technology Research Facility (ATRF) and Vaccine Pilot Plant (VPP) facilities, and access to buildings and rooms throughout the NCIF facilities located on Fort Detrick. Frederick PACS captures NCIF employee pictures as a way to identify employees that may have misplaced or lost their HHS Personal Identifiable Verification (PIV) badges.

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

The type of information that Frederick PACS collects and maintains include records on NCIF

employees, summer students, cafeteria workers, contractors who are issued HHS PIV cards, and vendors that support the NCIF. Personally Identifiable Information (PII) data includes name, work address or physical location address, email address, and a photo. Submission of this information is voluntary. However access to NCIF facilities requires a current and active HHS PIV Card. PII is extracted from the NIH Enterprise Directory (NED). NED maintains its own and unique Privacy Impact Assessment (PIA) on record, including all legal authorities documented.

Frederick PACS uses specific login information to assign permissions/user roles which is considered PII. However, this is done by using t 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.

The primary purpose of the Frederick PACS is to manage physical access to NCIF facilities, access through perimeter gates at the ATRF and VPP facilities, and access to buildings and rooms throughout the NCIF facilities located on Fort Detrick. Frederick PACS captures NCIF employee pictures as a way to identify employees that may have misplaced or lost their HHS PIV badges.

The type of information that Frederick PACS collects and maintains include records on NCIF employees, summer students, cafeteria workers, contractors who are issued HHS PIV cards, and vendors that support the NCIF. PII data includes name, work address or physical location address, email address, and a photo. Submission of this information is voluntary. However access to NCIF facilities requires a current and active HHS PIV Card. PII is extracted from the NED. NED maintains its own and unique PIA. PII is extracted from NED. NED maintains its own and unique PIA on record, including all legal authorities documented.

Frederick PACS uses specific login information to assign permissions/user roles which is considered PII. However, this is done by using t the NIH 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.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
Photographic Identifiers
E-Mail Address
Mailing Address
physical location and work address

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

Employees
Public Citizens
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The primary purpose of the PII used for Frederick PACS is to validate and authenticate identity in order to manage physical access to NCIF facilities, including access through the perimeter fences at the ATRF and VPP facilities, as well as access to buildings and room throughout the Fort Detrick campus.

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

N/A

Identify legal authorities governing information use and disclosure specific to the system and program.

5 U.S.C. 301; 5 U.S.C. 5901; 5 U.S.C. 7903; 40 U.S.C. 318a; 42 U.S.C. 241

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.

09-25-0054 Administration: Property Accounting (Card Key System) HHS/NIH/ORS

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within the OPDIV

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

1615-0047, E-Verify Employment Eligibility Verification, expiration date: 05/31/2027

3206-0182, Declaration for Federal Employment, expiration date: 08/31/2026

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.

Individuals are notified of the collection and use of the data as part of the hiring process. This is a requirement of all potential job applicants seeking employment at NIH. Individuals are informed that they need their picture taken at the time their HHS PIV Badge is encoded with appropriate NCIF locations/building access.

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.

There is no option to opt-out. The collection of PII is voluntary, however access to NCIF facilities requires a current and active HHS PIV Card. Individuals cannot access without the submission of their PII.

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

Current system users/administrators' PII is downloaded from NED. NED maintains its own and unique Privacy Impact Assessment (PIA) on record, including all legal authorities documented. Individuals are contacted via email if any changes are made or anticipated to the 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.

Individuals may contact the NCIF HelpDesk (fredhelpdesk@nih.gov) for any action.

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

PACS undergoes regular and periodic reviews. PII is only obtained when the HHS PIV badge is encoded for NCIF Building Location/Building access.

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 is limited by job role with approval by system owner or designated representative. Temporary access could be granted to troubleshoot specific issue such as a data integrity concerns. System users are approved by Frederick PACS' management for access based on their technical/functional role in administering, developing, and supporting the daily job functions of Fredereick PACS.

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.

Only authorized users are allowed in the system. Access to or change of specific PII fields is restricted to proper roles within the Frederick PACS system. There is a process in place to remove access when employee transfers/terminates.

A NIH IAM 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.

Describe training system users receive (above and beyond general security and privacy awareness training).

Users with additional roles for system administration, risk management, leadership, continuity of operations and safety receive additional training for ethics, equal opportunity and diversity, Notification and Federal Employee Anti-discrimination and Retaliation (No FEAR) Act, Green, and use of strategic sourcing.

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 according to NIH Record Retention Schedule.

Item 06-220, Hiring Manager, Office supervisory or Manager records (Onboarding, Offboarding and/or Transferring Employees)
Description: Hiring Manager, Office Supervisory or Manager records which capture Information pertaining to prospective and /or current employees, which may cover some of the same actions as those in the Official Personnel Folder maintained in the civilian personnel office. These records may be filed by employee name and contain complete employee information.
Disposition Instruction: Review annually and destroy superseded documents. Destroy remaining documents 1 year after employee separation or transfer.
Disposition Authority Agency (DAA): DAA-GRS-2017-0007-0012, GRS 2.2, item 80

Item 09-403: Key and card access accountability records. All other facility security areas.
Description: Key and card access accountability records. All other facility security areas. Records accounting for keys and electronic access cards. Includes areas designated by the Interagency Security Committee as Facility Security Levels I through IV.
Disposition Instruction: Destroy 6 months after return of key, but longer retention is authorized if required for business use.
Disposition Authority: DAA-GRS-2017-0006-0003

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

Administrative Controls: System users are approved by Frederic PACS' management for access based on their technical/functional role in administering, developing, and supporting Frederick PACS' daily job functions, and Frederick PACS administrators perform periodic reviews to assure users adhere to system policies.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.

Physical Controls: The servers reside in the ATRF and Bldg. 430 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.