# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

08/05/2025

### OPDIV:

NIH

### Name:

Physical Access Control System-Access Expert (PACS-AE)

**PIA Unique Identifier:**

P-4055946-348772

**The subject of this PIA is which of the following?**

Minor Application (child)

**Identify the Enterprise Performance Lifecycle Phase of the system.**

Development

**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?**

New

**Does the system have Security Authorization (SA)?**

No

**Indicate the following reason(s) for updating this PIA.**

**Describe the purpose of the system.**

The NIH Physical Access Control System - Access Expert (PACS-AE) is the access control system for physical access to NIH facilities. This includes access to the NIH main campus and to buildings and rooms throughout the NIH main campus enclave, Rocky Mountain Laboratories (RML), and the Integrated Research Facilities (IRF). The PACS-AE system protects critical assets, including Biosafety labs (BSL-4), Select Agent labs, Irradiator rooms, Pharmaceuticals, and financial handling areas. The PACS-AE system is necessary to ensure NIH’s compliance with certain regulatory requirements.

In addition, PACS-AE receives information from NIH Enterprise Directory (NED) and Human and Health Services (HHS) Smart Card Management System (SCMS) required to provision physical access to NIH employees and direct contractors, volunteers, retirees, extended visitors, special government employees (NIH board members) and service providers.

Extended Visitor Badges are issued after the visitor completes the "Extended Visitors Form" and

Patient/Patient Visitors use the "Clinical Center Patient and Patient Visitor Form". The Division of Police (DP) have access to the PACS-AE workstations. The PACS-AE application prompts the DP for the visitors First Name, Last Name, and Expiration Date required for the 1-year extended visitor badge. Once the information is input, the Division of Personnel Security (DPS) Badge Administrator completes the badge process by taking the visitor's photo and printing the badge from the PACS-AE workstation.

Extended Visitors Process: DP and DPS Badge Administrators support the Extended Visitors & Patient/Patient Visitors process (facnet 38-workstations).

Employee/Contractor Process: The DPS Badge Administrators use the Enrollment & Issuance workstations for PIV cards and HHS-Issued IDs. (nihnet workstations).

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

The PACS-AE collects, maintains, and shares the following personally identifiable information (PII): Full name, work address, email, phone number, badge photo, fingerprints, HHS Personal Identity Verification (PIV) card numbers, Operating Division (OpDiv) Name, employment status, and Federal Agency Smart Credential Number (FASC-N), including card expiration date, username, and personal identification number (PIN). Data is collected for all NIH federal employees and direct contractors. Data is derived from NIH Enterprise Directory (NED) and Human and Health Services (HHS) Smart Card Management System (SCMS) through the Physical Access Control System Integrated System (PACSIS) middleware. NED, SCMS and PACSIS maintain their own Privacy Impact Assessments (PIAs), including all legal authorities documented.

NIH employees log into the 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.**

The NIH PACS-AE is the access control system for physical access to NIH facilities. This includes access to the NIH main campus and to buildings and rooms throughout the NIH main campus enclave, RML, and the IRF. The PACS-AE system protects critical assets, including Biosafety labs (BSL-4), Select Agent labs, Irradiator rooms, Pharmaceuticals, and financial handling areas. The PACS-AE system is necessary to ensure NIH’s compliance with certain regulatory requirements.

In addition, PACS-AE receives information from NED and HHS SCMS required to provision physical access to NIH employees and direct contractors, volunteers, retirees, extended visitors, special government employees (NIH board members) and service providers.

Extended Visitor Badges are issued after the visitor completes the "Extended Visitors Form" & Patient/Patient Visitors use the "Clinical Center Patient and Patient Visitor Form". The DP have access to the PACS-AE workstations. The PACS-AE application prompts the DP for the visitors First Name, Last Name, and Expiration Date required for the 1-year extended visitor badge. Once the information is input, the DPS Badge Administrator completes the badge process by taking the visitor's photo and printing the badge from the issuance workstation.

Extended Visitors Process: DP and DPS Badge Administrators support the Extended Visitors and Patient/Patient Visitors process (facnet 38-workstations).

Employee/Contractor Process: The DPS Badge Administrators use the Enrollment & Issuance workstations for PIV cards, HHS-Issued, IDs. (nihnet workstations).

The PACS-AE collects, maintains, and shares the following PII: Full name, work address, email, phone number, badge photo, fingerprints, HHS PIV card numbers, OpDiv Name, employment status, and FASC-N, including card expiration date, username, and PIN. Data is collected for all NIH federal employees and direct contractors. Data is derived from NIH Enterprise Directory (NED) and Human and Health Services (HHS) Smart Card Management System (SCMS) through the PACSIS middleware. NED and PACSIS maintain their own PIAs, including all legal authorities documented.

NIH employees log into the system using 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
Biometric Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Employment Status
PIV card number
OpDiv Name
FASC-N card expiration date, username and PIN

**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
Volunteers, retirees, extended visitors, special government employees (NIH board members), service providers.

**How many individuals' PII is in the system?**

50,000-99,999

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

The primary purpose of the PII is to validate and authenticate identity in order to manage physical access to NIH facilities, including access through NIH main campus, buildings and rooms throughout the NIH main campus enclave, Rocky Mountain Laboratories (RML), and the Integrated Research Facilities.

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

PACS-AE is also used as an application to process information and PII required to issue HHS PIV cards to badge holders.

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

40 U.S.C. 318a; 42 U.S.C. 241, 42 U.S.C. 281 and 42 USC 282

**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.**

09-90-0777, Facility and Resource Access Control Records

09-25-0216, Administration: NIH Enterprise Directory

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

Other HHS OPDIV

Non-Government Sources

Public

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

OMB information collection approval is not required for federal employees. Information that is collected from public citizens, is exempt because the information is used solely to self identify and grant access to NIH premises.

**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.**

Several Interconnection Security Agreements (ISA) exist with Center for Information Technology (CIT) for the secure connection to HHS systems. Another ISA exists between NED for the secure connection to support the Homeland Security Presidential Directive (HSPD-12) PIV Production.

PACS-AE maintains ISA with:
NIH Enterprise Directory System (NED)
HHS Smart Card Management System (SCMS)
National Institute of Environmental Health Sciences (NIEHS)
National Cancer Institute (NCI)

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

For information within PACS-AE that is held in a system of records, an accounting of disclosures is developed and maintained, including the date, nature, purpose of each disclosure, and the name and address, or other contact information of the individual or organization to which the disclosure was made. PACS-AE retains the accounting of disclosures for the length of time the PII is maintained or five years after the disclosure is made, whichever is longer. PACS-AE makes the accounting of disclosures available to the

individual to whom the PII relates upon request.

**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 understand they are required to provide their information as part of the onboarding process. This is stated during the completion of the electronic questionnaires profile, using the National Background Investigation Services eApplication (eApp), including the provision of background information. eApp is a web-based automated system used in collecting information from individuals for employment background investigation.

Extended Visitors use the "Extended Visitors Form" & Patient/Patient Visitors use the "Clinical Center Patient and Patient Visitor Form" to apply for 1-year Physical Access to the NIH campus.

**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.**

Employee's/Contractor's PII is derived from NED and therefore there is no opt-out option. The information collection is required as part of the hiring process. NED maintains its own PIA, including all legal authorities. Visitors cannot opt out because the PII is required to grant the extended visitor badge necessary to access the campus facility and/or doors/labs.

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

Information that is pulled from the NED have its own PIA and process for notifying individuals when changes to the system occur. NED maintain its own approved PIA, with process in place to notify individuals that their PII will be collected.

Extended Visitors use the "Extended Visitors Form" & Patient/Patient Visitors use the "Clinical Center Patient and Patient Visitor Form" to apply for 1-year Physical Access to the NIH campus.

**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 NIH Information Technology (IT) Service Desk and if necessary, a ticket is assigned to the PACS-AE operations and support team for action. For information that downloads from NED, individuals may also contact the NED team directly at nedteam@mail.nih.gov. An email request is planned for use to obtain individual consent. As such the NIH global email system is in place and capable of reaching NIH PIV card holders.

Extended Visitors who use the "Extended Visitors Form" & Patient/Patient Visitors use the "Clinical Center Patient and Patient Visitor Form" notify the DP to resolve the individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. The individual's information is corrected by DP within the PACS-AE.

**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-AE undergoes regular and periodic reviews. The PII is downloaded from NED is reviewed when HHS PIV cards also known as badges are renewed. The timeline for badge renewal depends upon the type of badge and typically ranges from one (1) year to five (5) years. Alternatively, individuals have the option to conduct ad hoc reviews of their own PII through NIH NED Self Service.

Information that is collected from the Extended Visitor's forms is saved with an expiration date. Once reached, the card status is automatically disabled. In addition, PACS personnel periodically reviews list of individuals being identified as inactive and manually validates that the card status is changed to disabled and remove the individual's physical access to the NIH campus.

**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.**

Information system users are approved by PACS-AE management for access based on their technical/functional role in administering, developing, and supporting the daily job functions of PACS-AE.

**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.**

Annual review of system users' roles are done to assure access is current with user's technical/functional role in administering, developing, and supporting the daily job functions of PACS-AE.

**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).**

Application specific training is provided by the system owner or experienced super users.

**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.**

07-105: Information technology (IT) operations and maintenance records. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use. (DAA-GRS-2013-0005-0004).

07-204: System access records. Systems requiring special accountability for access. 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).

07-211: Public Key Infrastructure (PKI) transaction-specific records. Destroy/delete when 7 years 6 months to 20 years 6 months old. Longer retention is authorized if the agency determines that transaction-specific PKI records are needed for a longer period. (N1-GRS-07-3, item 13b).

09-403: Key and card access accountability records. All other facility security areas. Destroy 6 months after return of key, but longer retention is authorized if required for business use. (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.**

Physical Controls: The information technology (IT) hardware used to host protected information is located in a secured data center facility within Amazon Web Services (AWS) Government Cloud. 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.