US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/25/2016

OPDIV:

OS

Name:

PACSNorth1

PIA Unique Identifier:

P-5255687-545261

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?

Yes

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.

N/A

Describe the purpose of the system.

Physical Access Control System North1 (PACSNorth1) is an access control application designed to grant, monitor, and maintain physical access of individuals to the Parklawn Building and the connected complex in Rockville MD.

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

The information in the system is maintained for the purpose of granting physical access of individuals to the Parklawn Building and the connected complex in Rockville MD. PACSNorth1 collects and maintains personally identifiable information (name, photo, employee office location, employee number (Personal Identifier), and Federal Agency Smart Credential Number (FASC-N)) for the purpose of printing PIV (Personal Identity Verification) cards and generating access requests.

In order to be granted the appropriate request, each individual (Federal employee & direct contractor) is required to submit this personal information at the time employment is accepted as part of the on-boarding process via Form 828. The FASC-N is generated when the card is printed. PIV cards are not printed for non-federal visitors. Non-federal visitors are required to provide a photo ID which is used to print a temporary paper badge containing name and photo. This PII is stored for two years.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The PACSNorth1 system is an access control application designed to grant, monitor, and maintain physical access to the Parklawn Building and the connected complex in Rockville MD. PACSNorth1 collects and maintains personally identifiable information (name, photo, employee office location, employee number (Personal Identifier), and Federal Agency Smart Credential Number (FASC-N)) for the purpose of printing Personal Identity Verification (PIV) cards and generating access requests. This occurs by comparing the PII encoded into PIV cards with information contained within HHS's Smart Card Management System (SCMS) (aka Identity and Access Management System (IAMS)), to which PACSNorth1 is connected. Users swipe their PIV card, and that information is validated by PACSNorth1. If necessary, individuals can be directed to a booth where a temporary paper badge, containing name and photo only, can be created; also using PACSNorth1. PII is submitted by the employees themselves as part of the on-boarding process. Non-federal visitors are required to provide a photo ID which is used to print a temporary paper badge containing name and photo only. PACSNorth1 also records "events" (irregularities) and provides alarms (notifications where access authorization appears incorrect or inappropriate).

No reports containing PII are generated from the PACSNorth1 system.

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

Federal Agency Smart Credential Number (FASC-N)

Employee Number (Personal Identifier)

Employee Office Location

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

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

Information is used to confirm identity and to verify the PIV card/badge holder has permission to enter certain HHS facilities.

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

PII is not used for secondary purposes.

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

Primarily Homeland Security Presidential Directive 12 (HSPD-12) calls for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and to the employees of federal contractors. Agencies must ensure consistency with existing privacy and security law and policies to ensure employee and contractor information is protected and appropriately used. Additional legal authorities include: HHS-Office of the Chief Information Officer (OCIO) Policy for Privacy Impact Assessments, 2/9/09, Federal Information Processing Standard (FIPS) 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Security Management Act of 2002 (FISMA), and Office of Management and Budget (OMB) Circular No. A-130. SORN 09-90-0777: U.S.C. 301 Information Technology Management Reform Act 1996 (pub. L. 104-106, sec.5113) and Privacy Act of 1974, 5 U.S.C. 552a(b).

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.

Facility and Resource Access Control Records 09-90-0777

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Government Sources

Other HHS OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

N/A

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 aware of what PII is collected because they either supply it themselves directly or because the use of the information is implicit in the employer/employee relationship. There is a Privacy Statement associated with the collection of this information that is signed by the individual before the information is released. The Privacy Statement explains to the individuals the purpose for the collection of this information, the authority for the collection, with whom the information is shared, and how they can receive an accounting of disclosures.

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.

Information is collected directly from individuals. Consent is granted as part of the employee (Federal & direct contractor) on-boarding process via Form 828.

Although the use of PII is implicit in the employer/employee relationship, and for all those entering the facilities, a SORN is required under the Privacy Act, and will be used to describe any use of an Individual's PII for purposes materially different from that given at the time of collection.

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

Individuals would be notified via email of major system changes that affect their rights or interests. Major changes would also be reflected by updates to the system of records notice (SORN).

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 who believe their PII is inaccurate or incomplete can contact the Help Desk or otherwise identify the appropriate system owner to correct or amend the information.

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 (PII) resides in Identity and Access Management System (IAMS), which is updated periodically. PACSNorth1 downloads information from IAMS to a LENEL OnGuard database. LENEL is the brand name of the access control database used by PACSNorth1.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Access to PII available based on rights assigned by the Administrators. Necessary for assigning access rights to HHS occupied buildings. Users have different levels of access based on their role and duties.

Administrators:

Responsible for assigning access rights to other users.

Developers:

Full access to system. Responsible for application updates.

Contractors:

Full access to system. These direct contractors are responsible for application updates, data base administration, and system administration.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Administrators, developers, and direct contractors have access to PII. Access levels are provided and restricted based on the user's role and/or time constraint. Access is repealed via receipt of an e-mail request from authorized management staff.

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.

The PACSNorth1 system is segmented which means those with access ("the User") are restricted to accessing the record of all individuals in their segment. In addition, the "Users" are assigned access levels which restrict their ability to view records based on the User's role and responsibilities.

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.

The Office of Security and Strategic Information (OSSI) complies with the FISMA requirement to be exposed to security awareness materials, at least annually and prior to employee's use of, or access to, information systems by communicating directly with individuals who access the system. This training includes the annual HHS Privacy and Security Awareness training.

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

In addition to the general security and privacy awareness training, system users receive on the job training.

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.

National Archives and Records Retention guidelines (GRS24) permit retention of the data for several years, but PACSNorth1 only retains the data as long as it is current. When there are employment status changes, data is removed from the LENEL database.

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

PII is secured using:

Administrative controls include roles and responsibilities to provide for access using the concepts of least privileges and separation of duties. Access levels are provided and restricted based on the user's role and responsibilities. Certification and accreditation activities are performed to ensure security controls are in place and operating as designed. Also the PACSNorth1 system is segmented which means those with access ("the User") are restricted to accessing the record of all individuals in their segment.

Technical controls are in place to limit access to only those requiring it and only for those purposes intended and authorized by the System Owner. These include UserID, password, IDS (Intrusion Detection System) and firewalls.

Physical controls to the system are provided by the Office of Information Technology Infrastructure and Operations (ITIO) and include security guards, ID badges, key cards, cipher locks and Closed-Circuit TV (CCTV).