US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/02/2024

OPDIV:

NIH

Name:

Visitor Badging System

PIA Unique Identifier:

P-7210182-789366

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

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

The Visitor Badging System (VBS) has incorporated the usage of the EntryPoint preregistration portal module. This module consists of a private web registration request form that a National Institutes of Health (NIH) sponsor will request to be forwarded to a visitor to access NIH campus. This web registration form is directed specifically to the visitor and upon its completion and submittal, the web form Uniform Resource Locator (URL) will expire and no longer be accessible.

Describe the purpose of the system.

The Visitor Badging System (VBS) application acts as a badge issuance system for visitors to National Institutes of Health (NIH) facilities. The EntryPoint preregistration portal module is a service that allows NIH sponsors to forward a short lived web page to the visitor to complete registration requirements and send back to NIH for review. Once theweb form is completed and sent to NIH, the Uniform Resource Locator (URL) and webpage will expire and will no longer be usable.

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

The VBS collects name, address, date of birth, place of birth, passport number, license number, vehicle identifiers, phone numbers, and photo identification. The printed identification card contains their name, photo, and the current date.

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 names and passwords (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 VBS application acts as a badge issuance system for visitors to most NIH facilities.

The VBS collects name, address, birth date, place of birth, passport number, license number, vehicle identifiers, phone numbers, and photo identification. The printed identification card contains their name, photo, and the current date.

Users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own 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 names and passwords (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.

Date of Birth
Name
Photographic Identifiers
Driver's License Number
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Passport Number
Place of birth
Current date

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?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of PII used by VBS is to verify identity of visitors to the NIH and control Personal Identity Verification (PIV) cards and identity credentials issued to persons entering and exiting the facilities.

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; Information Technology Management Reform Act of 1996 (Pub. L. 104-106, sec. 5113); Federal Information Security Management Act of 2002 (44 U.S.C. 3554); Electronic Government Act (Pub. L. 104- 347, sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. . 3501 et al); Government Paperwork Elimination Act (Pub. L. 105-277, sec. 1701, 44 U.S.C. 3504); Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, Aug. 27, 2004; Federal Property and Administrative Act of 1949, as amended.

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.

GSA/GOVT-7 HSPD-12 USAccess

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within the OMB

Other HHS Operating Divisions

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

0925-0177; Expiration Date: 03/31/2026

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.

Visitors are directed to the NIH Visitor Information site where they are informed of what information is required for visitors that seek access to NIH facilities.

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.

The VBS requires PII collection to validate an individuals identity, mitigate risk, and support the access security and safety mission of the NIH. Individuals have the ability to opt-out of giving their PII, but this will negate their ability to enter the NIH campus.

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

Individuals may contact the NIH Visitor Center at 301-496-1776 if they have questions about their information.

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.

If individuals believe that their information has been compromised or inappropriately used/obtained/disclosed, may contact the NIH Visitor Center at 301-496-1776.

There is no process to obtain consent from the individuals whose PII is stored in VBS. The system is the last step in obtaining a visitor's badge.

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

VBS has annual reviews of PII contained in the system, as well as audits of data logs to assure all information is accurate and relevant.

When a visitor returns to the NIH, the system will automatically connect the new visit with the records of the visitor. If it isn't a clear match (different ID, such as passport instead of previous driver's license), the system will notify the guard to manually verify if the individual matches the suggested prior visitor or is the individual a new visitor.

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.

The procedure to determine which system users may access PII is granted through a request to the system owner. Along with a proper reason for needing access to the PII.

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.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles and the principle of least privilege. Authentication with NIH Personal Identity Verification (PIV) card will occur at time of login to the NIH Network.

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 NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel (employees and direct contractors) who use NIH applications must complete security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid credentials.

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

All users receive in-person training on how to operate the system during the registration process.

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 maintained and destroyed in accordance with NIH record retention schedules:

09-401, Security administrative records: Security management administrative records. Records about routine facility security, protective services, and personnel security program administration not covered elsewhere in this schedule. Disposition Instruction: Destroy when 3 years old, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS-2021-0001-000.

09-412, Facility security management operations records: Records about detecting potential security risks, threats, or prohibited items carried onto federal property or impacting assets.
Disposition Instruction: Destroy when 30 days old, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS-2021-0001-0003

09-414, Visitor processing records. Areas requiring highest level security awareness: Registers or logs recording names of outside contractors, service personnel, foreign national and other visitors, employees admitted to areas, and reports on vehicles and passengers.
Disposition Instruction: Destroy when 5 years old, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS-2017-0006-0014.

09-415, Visitor processing records: All other facility security areas. Registers or logs recording names of outside contractors, service personnel, foreign national and other visitors, employees admitted to areas, and reports on vehicles and passengers.
Disposition Instruction: Destroy when 2 years old, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS-2017-0006-0014.

09-417, Personal identification credentials and cards: Records about credential badges that are based on the Homeland Security Presidential Directive (HSPD-12) standards for identification cards issued to Federal employees, contractors, and affiliates.
Disposition Instruction: Destroy after expiration, confiscation, or return. Disposition Authority: DAA-GRS-2017-0006-0017.

09-418, Temporary and local facility identification and card access records: Temporary employee, contractor, and occasional visitor facility and network identification access card and identity management system records.
Disposition Instruction: Destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS-2021-0001-0006.

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.