US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/17/2016

OPDIV:

OS

Name:

HHS Foreign National Management System

PIA Unique Identifier:

P-4801246-566803

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Test

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?

Yes

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 Foreign National Management System (FNMS) is an enterprise wide web application used by Health and Human Services (HHS) Operating Divisions (OpDivs) and Staffing Divisions (StaffDivs) to enter and track foreign national visits to HHS facilities worldwide. FNMS will collect and maintain the following personally identifiable information (PII) data for foreign nationals:

First and Last Name
Date of birth
Gender
Birth Location (Country/Province/State)
Phone Number
Mailing address
Email address
Photographic Identifier
Passport Number
Visa Information

The PII is collected once a Foreign Visitor initiates a request to visit an HHS facility.

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

Once a Foreign Visitor decides to visit an HHS facility, a Requester initiates the visit request. The Requester is an HHS Staff member requesting the Foreign Visitor be permitted to visit HHS facilities. If a Requester has an account in FNMS, the Requester logs into FNMS and submits a visit request. If the Requester does not have an account in FNMS, the Requester must first contact the Office of Security and Strategic Information (OSSI) or the FNMS Helpdesk to request access. The FNMS Access request form is provided via email to the requestor; once the Requester completes the FNMS Access Request Form they will submit the completed form to the Office of Enterprise Application and Development (OEAD) via email. The access request form contains the following PII data elements: First Name, Last Name, email, phone number. Upon receipt and review, OEAD will create a new account for the user. After the new account is created, FNMS will send the new user an email welcoming them to FNMS. The welcome email will contain the user's login name, a link to FNMS, and instructions on how to obtain their password. After completing the indicated steps and receiving their password, the new user logs in to FNMS and submits the visit request. Next, the Requester assigns a Host and an Escort for each visit made by the Foreign Visitor.

The Host assumes responsibility for the Foreign Visitor while present on HHS grounds. The Escort is responsible for accompanying the Foreign Visitor while accessing HHS facilities, maintaining visual and voice contact at all times in all non-escort free areas or areas to which the Foreign Visitor is not permitted independent access. Next, an FNMS Approver is responsible for reviewing a Foreign Visitor's documentation and approving access to the requested HHS facility. An FNMS Guard is responsible for checking the Foreign Visitor in once they arrive at their point of entry. The FNMS Guard can view all visitor information and filter visitors by status to see other visitors in addition to those approved by the FNMS Approver. FNMS will collect and maintain the following personally identifiable information (PII) data for foreign nationals:
First and Last Name
Date of birth
Gender
Birth Location (Country/Province/State)
Phone Number
Mailing address
Email address
Photographic Identifier
Passport Number
Visa Information

The PII is collected once a Foreign Visitor initiates a request to visit an HHS facility. After this, the Requester assigns a Host and an Escort for each visit by the Foreign Visitor. The Host assumes responsibility for the Foreign Visitor while present on HHS grounds.
FNMS will collect and maintain the following personally identifiable information (PII) for the following roles requester, host, approvers, FNMS guards, guards and escorts:
First Name
Last Name
Phone Number
Email Address
Employment Status (Federal Employee/Contractor)
Agency/Sub Agency/Division
User credentials (email address and password) will be stored in FMNS for HHS employees and direct contractors for the purpose of system access.

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

FNMS is the system used by HHS OpDiv and StaffDivs to enter and track foreign visitors to HHS facilities worldwide. The PII collected, as referenced above, will be collected when a request is made for a Foreign Visitor to visit an HHS facility. PII of foreign visitors and HHS personnel will be stored for 10 years after a foreign national visit; or 10 years after a visitor's account is disabled. The Foreign Visitor's information will not be shared unless authorized law enforcement request access.
The PII is collected once a Foreign Visitor initiates a request to visit an HHS facility. After this, the Requester assigns a Host and an Escort for each visit by the Foreign Visitor. The Host assumes responsibility for the Foreign Visitor while present on HHS grounds.

An Escort is responsible for accompanying the Foreign Visitor while accessing HHS facilities, maintaining visual and voice contact at all times in all non-escort free areas or areas to which the Foreign Visitor is not permitted independent access. Next, an FNMS Approver is responsible for approving access to the requested HHS facility. An FNMS Guard is responsible for checking the Foreign Visitor in once they arrive at their point of entry. The FNMS Guard can view all visitor information and filter visitors by status to see other visitors in addition to those approved by FNMS Approver.

Once PII data is received by a Foreign Visitor, it is not transmitted or shared outside of HHS unless requested by authorized law enforcement and intelligence communities to protect HHS personnel, information and assets in order to meet the requirements of numerous laws, orders, policies, and regulations.

PII is shared within HHS when the Requester has to initiate a visit request and does not have an FNMS account. The Requester must first contact the Office of Security and Strategic Information (OSSI) to request access. The Requester completes the FNMS Access Request Form (currently in draft) and submits to OSSI. OSSI will review the form and if they approve, OSSI will send the approved form to the Office of Enterprise Application Development (OEAD). Upon receipt, OEAD will create a new account for the user.

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

E-Mail Address

Mailing Address

Phone Numbers

Employment Status

Passport Number

Agency/ Sub Agency/Division for the roles of requestor, host, approvers, FNMS Guards, Guards and

Gender
Visa Information
Birth Location: Country/Province/State
HHS User Credentials (email address and password)
Employment Category (Federal Employee or Contractor)

Birth Location: Country/Province/State

HHS User Credentials (email address and password)

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

Foreign Nationals

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of the PII will be to identify and validate foreign visitor's access to HHS facilities.

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

There are no secondary uses of PII.

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

The implementation of this system, including activities such as the collection of PII necessary for operating it, are authorized by 5 U.S.C. 301. 42 U.S.C § 3502 creates the Office of the Assistant Secretary for Administration (ASA) at HHS, and among the duties delegated to the ASA are oversight of these services, which are necessary to developing and maintaining a workforce.

31 U.S.C. 66a; 5 U.S.C. 5501 et seq., 5525 et seq., 5701 et seq., and 6301 et seq.; Executive Order 9397; Pub. L. 100–202, Pub. L. 100–440, and Pub. L. 101–509

Also, FNMS allows HHS to meet the requirements of Presidential Policy Directive (PPD) -21, the Counterintelligence Enhancement Act of 2002, and Executive Order 13587 – National Insider Threat Policy.

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 & Resource Access Control Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

Because FNMS does not collect PII from members of the general public, an OMB information collection approval number and expiration date is not applicable.

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.

Prior to arriving at HHS, a Foreign Visitor will receive a system generated email requesting them to access the FNMS system and provide personal information. Upon accessing the site, a disclosure statement is displayed informing the Foreign Visitor that providing personal information is voluntary and is needed prior to visiting any HHS facility. Since this information is voluntarily submitted, the Foreign Visitor is aware of the information being collected.

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 for a Foreign Visitor to opt-out of the collection of their PII if they desire to visit a HHS facility. The individual must understand that they must be identified and their information validated in order to gain access. Individuals will have awareness of how their information will be used. In the event a visitor decides to opt-out of providing PII they will not be granted access to HHS facilities.

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

The System of Record Notice (SORN) describes some of the ways the records will be used within the agency and some of the reasons why the records may be disclosed to parties outside the agency. If the system changes in a way that will conflict with the SORN, a new or revised SORN will be published in the Federal Register providing a 30-day public notice comment period.

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.

An individual can contact HHS' Office of Public Affairs if they believe their PII has been inappropriately obtained, used, or disclosed at the following website: www.hhs.gov.

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

On an annual basis the current list of users will be provided to the business owner (OSSI) for review and validation. The list will be provided through a secured method, in accordance with HHS security guidance. The FNMS system owner (OEAD) will make necessary updates as requested by business owner (OSSI).

Foreign national's PII are not reviewed periodically to ensure the data's integrity, availability, accuracy and relevancy. The PII for the the foreign national is only validated during the scheduled visit. In event a foreign national revisits a HHS facility the visitor will be required to resubmit their PII for the new visit.

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

Users:

HHS Designated users have role-based access to information depending on which OPDiv or StaffDiv they work for, and their job function and appropriate documentation.

Administrators:

Application Administrators in the chain of command grant approval for requested role-based access received through a user provisioning system.

Developers:

Developers respond to requests to add functionalities or make other changes to the system’s code or configuration.

Contractors:

May develop code if code or configuration changes are needed.

Others:

Requesters, Approvers, and FNMS Guards require PII access because the Requester is responsible for completing the request form for the foreign national. The Approver is responsible for approving access to HHS facilities. The FNMS Guard checks the foreign national visitor in upon arrival at point of entry.

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

The FNMS will be used by HHS OPDivs and StaffDivs to enter and track Foreign Visitors accessing HHS facilities. Specifically, PII data will be accessed by the Requester, Approver and FNMS Guards. PII is not shared outside of HHS unless requested by authorized law enforcement and intelligence communities to protect HHS personnel, information and assets in order to meet the requirements of laws, orders, policies and regulations. FNMS access is restricted using a role-based authorization process. Only privileged users with administrative rights can access 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.

Access rights are determined by need to know basis when the user requests access. An annual recertification process is conducted to make sure user roles have not changed.
The current recertification process in place states that there will be a system generated email that will be sent to all user accounts requesting them to recertify by email to OSSI that they still have a role that requires access to FNMS. OSSI will review accounts and roles and provide the responses to OEAD with any modifications to the list of users and associated roles.

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.

Information Systems Security Awareness and Privacy Awareness trainings are required annually. In addition, the HHS Rules of Behavior must be acknowledged and signed before access is granted.

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

FNMS training is offered by HHS' Office of Enterprise Application Development (OEAD) staff.

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.

The scheduling and retention of data collected is a requirement for the FNMS system under the HHS Records Management and Disposition guidelines. The records will be retained and disposed of in accordance with National Archives and Records Administration's (NARA) General Records Schedule 2 (GRS 2).

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

The following administrative, technical, and physical controls are in place for FNMS:

Administrative Controls:
System security plan
Contingency (or backup) plan
File backup
Backup files stored offsite
User manuals
Security Awareness
Training
Contractor Agreements
Least Privilege Access
PII Policies

Technical Controls:
User Identification
Passwords
Firewall
Encryption
Intrusion Detection System (IDS)

Physical Controls:
Guards
Identification Badges
Key Cards

The system is secured by methods prescribed in the System Security Plan (SSP). The SSP calls for system life-cycle practices for federal systems. The methods employed include risk assessments and implementation of management, operational, and technical controls.

In the Security Authorization process; National Institutes of Standards and Technology 800-53 Rev. 4 security controls and established the required level of security measures, including end user IDs, passwords, group accounts, a certified facility, background screening on system administrators will be utilized. The security controls will be reviewed annually, at a minimum.

Identify the publicly-available URL:

https://fnmsform.hhs.gov

The publicly available URL is only active and available to the user who received the email invitation from FNMS. FNMS generates a unique identifier per visitor which is included in the URL.

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

No

Does the website use web measurement and customization technology?

No

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null