US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/18/2016

OPDIV:

OS

Name:

Employee Eligibility System

PIA Unique Identifier:

P-3854101-286875

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?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

The purpose of Employee Eligibility System (EES) is to collect information from Federal Occupational Health (FOH) customers regarding their Federal employees that are eligible for work life services. The file that the agency customers provide contains the following information regarding Federal employees: employee ID, first name, middle name, last name, government email address, and date of birth. Fields that can be voluntarily submitted are: home address, phone number, site code (designates applicable agency, agency building or agency office region), HR (Human Resource) indicator (to provide required reporting), agency and building ID (To provide required reporting), gender. The work life services available to these employees is information regarding but not limited to: pregnancy, adoption, health issues and financial information.

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

EES stores eligible employee information as received from human resource systems across the federal government. This information is used for validation of eligibility for FOH and wellness program services.

The EES file includes the following information regarding Federal employees: employee ID, first name, middle name, last name, government email address, and date of birth. Fields that can be voluntarily submitted are: home address, phone number, site code (designates applicable agency, agency building or agency office region), HR (Human Resource) indicator (to provide required reporting), agency and building ID (To provide required reporting), gender.

Users connection and login to the Secure File Transfer Protocol (SFTP) server is controlled using a registered source Internet Protocol (IP) Address and key certificate authentication. The engineer uses their HHS credentials (username and password) to access the system.

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

Human Resource (HR) personnel from the following federal agencies: Department of Navy Civilian Employee Assistance Program (DONCEAP), General Services Administration (GSA) and Department of Energy Headquarters upload personnel records into EES for the purpose of identifying Federal employees that are eligible for Work life services. The record contains the following information Federal employees: employee ID, first name, middle name, last name, government email address, and date of birth. Fields that can be voluntarily submitted are: home address, phone number, site code (designates applicable agency, agency building or agency office region), HR (Human Resource) indicator (to provide required reporting), agency and building ID (To provide required reporting), gender.

Once the file has been successfully uploaded into EES, the Occupational Health Information System Security Engineer reviews the files for errors. Once the review is complete, EES will send a file status notification to the customer agency Point of contact (POC) via email and the engineer sends the file encrypted to the Contractor Owned Contractor Operated system vendor that is responsible for the Worklife4you system which has a separate privacy impact assessment. Upon successful transfer of the eligibility file, an email notification is sent to the occupational health and wellness program service provider POC.

Users connection and login to the SFTP server is controlled using a registered source IP Address and key certificate authentication. The engineer uses their HHS credentials (username and password) to access the system.

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

E-Mail Address

Mailing Address

Phone Numbers

Medical Notes

Employee ID

Other optional information: Gender, Agency and building ID, HR indicator and site code (signifies agency, agency building or agency office region)
User Credentials (username and password)

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

In cases where employees are seeking information about the care of their children or elder care, the name of their dependents may also be recorded in the system.

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Information is used to verify customer eligibility for services (for the care referral services) or to customize the user experience (for the health assessment services).

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

N/A The data is not used in any other capacity

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

FOH performs services under inter-agency agreements that are pursuant to 5 U.S.C. §7901 – Health Services Programs (PL 79-658). This statute authorizes the heads of agencies to establish health services programs for their employees.

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.

09-90-0018 - Personnel Records in Operating Offices

General Personnel Records OPM/Gov-1

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

This program does not collect information directly from the public, and therefore, is not subject to the requirements of the Paperwork Reduction Act.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

FOH receives information from their customers regarding specific staff that is eligible for FOH services

Other Federal Agencies

FOH receives information from their customers regarding specific staff that is eligible for FOH services

Private Sector

Contractor owned contractor operated system that provide the applicable Federal occupational health services receive the federal employee eligibility file from FOH which identifies the FOH customers staff that is eligible for FOH services. This is a separate company that has a contract to provide these services to Federal Employees

Describe any agreements in place that authorizes the information sharing or disclosure.

Each customer agreement has an individual inter-agency agreement with FOH. Agencies that elect FOH services complete an inter-agency agreement. The agreement will contain the FOH services that a particular agency decides to offer to its staff.

Describe the procedures for accounting for disclosures.

The Occupational Health Information System Security Engineer receives the SFTP sent from agencies. The engineer reviewed the file for any errors. If there are no errors, the engineer sends the file to the Contractor Owned contractor operated system vendor. The engineer archives all files.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Consent for staff is implicit in the employer/employee relationship. PII is used or shared only to facilitate the performance of professional responsibilities (e.g., to permit generation of usage metrics for FOH services) and facilitate collaboration. Employee information is collected when hired and if the agency has an interagency agreement with Occupational Health to offer the applicable work life services to their employees then the active employees name will be included in EES.

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.

Employees do not have to sign up for the services if they do not want them. Even though their information is provided, if the employee does not initiate signing up for the service offered, they will not receive the service. The service offered is a work   life benefit that an agency would have entered into an agreement with FOH to offer their employees if interested.

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

In the event of major changes, FOH would provide e-mail notification to affected persons.

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.

Users can contact the FOH helpdesk in the event that they have any issues with the system. Once contacted the helpdesk will escalate the issue if someones data has been jeopardized to the HHS Computer Incident Response Center if necessary.

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

Annual system security assessments of this system are performed. The system has been through a security accreditation following NIST 800-53 guidelines, and has been independently been verified to provide data integrity and availability as required by the accreditation process on an annual basis, it is required to demonstrate to independent auditors that these capabilities are maintained.

The Security engineer tracks the receipt of all customer agency files on a monthly basis. If the data provided by the customer agency isn't accurate, once received by the contractor owned contractor operated system, system checks are performed for consistency and formatting purposes.

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

Users:

Human Resource Personnel that sent the file to FOH to make sure that there are no errors in the file on their end.

Administrators:

Administrators that review the SFTP file sent from the customer agency to make sure that there are no errors in the file and send the file to the Contractor owned contractor operated system vendor.

Contractors:

Contractor owned contractor operated system vendor staff that receive the file from FOH to ensure that there are no file errors on their end.

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

System owners and Administrators evaluate the role and "need to know" of each user to determine if a user, in the performance of their duties, needs access to PII, to which PII access is needed, and the level of access required to that 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.

As dictated by their job roles, users are given access only to the information they need to accomplish their tasks. At no point are users given the opportunity to access more information than is needed to perform their job.

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 HHS Office of the Secretary complies with the Federal Information Security Management Act’s (FISMA) requirement that all agencies require all system users (employees and contractors) to be exposed to security awareness materials, at least annually and prior to the employee's use of, or access to, information systems. Current trainings include Information System Security Awareness and Privacy Awareness Training.

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

Users with security or administrative jobs are required to take standard role based training as defined and provided by the Department of Health & Human Services.

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 Official Personnel Folder (OPF) is maintained for the period of the employee's service in the agency and is then, if in a paper format, transferred to the National Personnel Records Center for storage or, as appropriate, to the next employing Federal agency. If the OPF is maintained in an electronic format, the transfer and storage is in accordance with the OPM approved electronic system. Other records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration records schedules or destroyed when they have served their purpose or when the employee leaves the agency. The transfer occurs within 90 days of the individuals' separation. In the case of administrative need, a retired employee, or an employee who dies in service, the OPF is sent within 120 days. Destruction of the OPF is in accordance with General Records Schedule-1 (GRS-1) or GRS 20.

Records contained within the Central Personnel Data File (CPDF) and Enterprise Human Resource Integration (EHRI) (and in agency's automated personnel records) may be retained indefinitely as a basis for longitudinal work history statistical studies. After the disposition date in GRS-1 or GRS 20, such records should not be used in making decisions concerning employees.

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

Administrative Security - Segregation of duties supported by application level and role-based security measures. Personnel have access to only those applications and systems necessary to perform their job functions. All applications require the successful authentication of each user.

Technical Security - The user is allowed several attempts to login correctly prior to being locked-out of the workstation. The EES receives customer agency eligibility files via an SFTP server. Connection and login to the SFTP server is controlled using a registered source IP Address and public key infrastructure (PKI) certificate authentication. Each customer agency has its own individual account and file directory on the SFTP server.

At least once a month each customer agency will upload a new copy of its employee eligibility file to its directory. Each customer agency can only access or view its own file directory. The uploaded file is checked for errors and is then loaded into the EES database in the Service Tracking Management system (STM). When the error check is completed on the uploaded file by the Occupational Health Information Security Engineer, EES will send a file status notification to the customer agency POC via email. Then the engineer will encrypt the file and send it to the Contractor Owned contractor operated system, Worklife4you which has a separate privacy impact assessment.

Physical Security - Employees are required to provide their secure assigned method of entry access. Visitors are required to sign in and they are escorted at all times.