US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/21/2016

OPDIV:

OS

Name:

Worklife4you

PIA Unique Identifier:

P-1990312-798208

The subject of this PIA is which of the following?

Major Application

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?

Yes

Identify the operator.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

No

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

PIA Validation

Significant System Management Change

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

Changes to the WorkLife system include a new presentation layer which is an enhanced website display and a content management system which is a centrally located system that creates, edits, maintains or deletes content. There has been no change to the business rule engine, the systems that will store personally identifiable information (PII), or the data points contained within.

Describe the purpose of the system.

The WorkLife application is a contractor-supplied web portal that Federal employees and their family members (if interested) can access in order to manage their work and life responsibilities more effectively. The site includes a variety of interactive tools and features, such as: a searchable database of medical providers, articles, webinars, podcasts, audio/video tips, calculators, etc.

Information can be provided on local community resources based on each individual's situation. Ex. Information on adoption services. Educational services are offered for each of the following work/life areas including: childcare and parenting, health and wellness, adult care and aging, legal and financial matters, education, adoption, and daily life.

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

Information collected that is required from registered users (federal employees) include: first name, last name, date of birth, email address and employee ID. 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. In addition, medical notes which are optional. Medical notes can be input if the user wants to have information available in the event that they need it to reference a condition/symptoms that themselves or a family member may have when researching information.

Use of this service is offered as a benefit to federal employees, and its use and the submission of PII is entirely voluntary. Some PII, however, may be necessary to validate eligibility for some services. There is an eligibility file that is sent from the Federal Occupational Health (FOH) to Total Health Solutions (THS) Worklife via secure file transfer protocol (SFTP) that contains eligible employee's first name, last name, middle initial, employee ID, site code, agency and location. The secure file transfer protocol allows file transfer, file access and file management securely over reliable data streams. This allows Worklife to confirm that a member is eligible for this service based on the eligibility file. The developer and administrators credentials (user id and password are stored in the system (Worklife4you).

Family members must be invited by the eligible federal employee to use the service. They are invited via an email invite. The family members would be required to provide their eligible members email address so that it can be determined if the family member can use the service or not. If they can use the service, the family member will create their own user ID and password to access the service. The family members' credentials are stored in the system (Worklife4you).

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

Worklife4you is a web-enabled tool that is made available to multiple federal agencies through FOH. It is a contractor owned, contractor operated system. Federal employees and their family members (if applicable) may access the web site directly, or use a hotline known as Benefit Connection, which is staffed 24/7 by employees of the vendor. The vendor employees have access to the web tool and can use it to locate resources and will assess, educate and direct Federal employees and their family members (if applicable) to the work life programs and benefits that are most suitable for their specific situation.

The tool assists customers (federal employees and their dependents) who have needs related to childcare and parenting, health and wellness, adult care and aging, legal and financial matters, education, adoption, and daily life. Customers can review the Website directly, or contact the vendor's customer service reps to assist them in identifying work life resources concerning their needs.

Information collected that is required from federal employees if registering for service are: first name, last name, email address and employee id.

Fields that can be voluntarily submitted are: home address, phone number, site code (designates applicable agency, agency building or agency office region), HR indicator (to provide required reporting), agency and building ID (To provide required reporting), gender. In addition, medical notes which are optional. Medical notes can be input if the user wants to have information available in the event that they need it to reference a condition/symptoms that themselves or a family member may have when researching information.

Use of this service is offered as a benefit to federal employees, and its use and the submission of PII is entirely voluntary. Some PII, however, may be necessary to validate eligibility for some services. There is an eligibility file that is sent from FOH via secure SFTP that contains eligible employees first name, last name, middle initial, employee id, site code, agency and location. The system can confirm that a member is eligible for this service based on the eligibility file. The developer and administrators credentials (user id and password are stored in the system (Worklife4you). The contractors are not direct contractors.

Family members must be invited by the eligible federal employee to use the service. They are invited via an email invite. The family members would be required to provide their eligible members email address so that if can be determined if the family member can use the service or not. If they can use the service, the family member will create their own user id and password to access the service. The family members' credentials are stored in the system (Worklife4you).

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

Protected Health Information (PHI) may voluntarily be provided by users, but it is not required.

Employee ID is required.

Gender, Agency and building ID, HR indicator and site code

Family Member User Credentials (User ID and Password)

Developer and Administrator credentials (user id and password)

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

Employees

Public Citizens

Vendor/Suppliers/Contractors

In cases where employees are seeking information about the care of their children or eldercare, 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

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.

General Personnel Records OPM/Gov-1

Employee Assistance Program Records 09-90-0010

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Per conversation with Office Management and Budget (OMB) clearance staff, an OMB control number and expiration date is not required.

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 customers send FOH information regarding their staff members that are eligible for FOH services

Private Sector

Total Health Solutions Worklife is a contractor owned contractor operated system. The vendor receives the federal employee eligibility file from FOH which identifies the FOH customers staff that is eligible for FOH services.

The data center provider that maintains the production data center environment can see PII within the operating system, and the records management vendor stores and maintains any historical information.

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. Ex. a facility gym, medical staff on-site. Agencies that want this health and wellness service offered to their employees and their family members if interested are authorizing Occupational Health by signing the interagency agreement to share/disclose the employees information with Lifecare in the event that an employee is interested in the Worklife4you program. Agencies have to sign this agreement in order to receive this program for their employees. This agreement and the employees that use the program are put into the Service Tracking Management system which is a separate Privacy Impact Assessment which tracks employee usage and bills agencies for using this Occupational Health Service.

Describe the procedures for accounting for disclosures.

Disclosures from this system are unlikely to be made, except in furtherance of the primary purpose of the system. If any nonstandard disclosures were to be made for any unanticipated reason, such that the disclosure was not a routine use, the system owner would maintain a record of the disclosures with the required data elements (date of the disclosure, recipient of the disclosure including a mailing address, content of the disclosure, purpose of the disclosure) in a designated file.

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

Customers are aware of what PII is collected because they either supply it themselves directly on the web site or supply it to a vendor staff person directly.

Before signing up to use the system, customers are required to review a privacy policy. This policy has been approved for use by HHS's Office of General Counsel (OGC). If any agency asks to modify the notice, OGC must review and approve the modification. This notice provides full explanation of how any PII will be used.

The vendor does not disclose or share PII data. The privacy policy will be reviewed, adjusted and approved by Federal Occupational Health and/or FedStrive as requested.

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.

Use of the system is entirely voluntary, and is offered to certain federal employees as a benefit. Customers are not required to create an account or otherwise use the system if they choose not to. Also, links to the Privacy Policy and Terms of Use documents are available on every website page, and customers are fully informed of the implications of providing PII if they choose to do so.

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

Upon a major system change, the vendor will notify and obtain consent in two ways:

The vendor will notify the Contracting Officer's Representative (COR) about upcoming material changes to the WorkLife system.

In the event of material changes to the WorkLife system that affects an individual's terms and conditions of use, all individual registered users of the WorkLife system will be presented with a popup with the new terms and conditions which will seek consent before access is granted.

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.

The end user may alert the vendor (in writing, email or via telephone) via the Help Desk function which will initiate a case with the vendors Quality Assurance team who will follow the issue through to resolution. This may involve reaching out to FOH if the issue appears to be the result of a privacy or security incident.

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

Applications are designed to ensure that input data is reviewed for proper format (i.e., dates, gender, and other fields must be internally consistent and fit the correct format). For "perishable" values (demographic information that may change over time), such as zip codes, an attempt is made to reconcile the data with other sources, e.g., zip codes are checked against addresses to see if they match.

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

Users:

Help Desk questions , Service Provider referral and case materials

Administrators:

Data loads, backups

Developers:

Limited as applicable for system defect diagnosis

Contractors:

Total Health Solutions Worklife is a contractor owned contractor operated system, as such the users, administrators and developers identified are affiliated with the vendor. These are not direct contractors.

Others:

Suppliers and Vendors that have access are the production data center vendor which maintains the production data center environment for Worklife4you and the records management vendor that stores and maintains any historical information.

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

Only staff with a current "need to know" are granted access. This need is validated at the time of requesting and granting an account, and assigning the access role(s). Requests for access are submitted into a centralized Online request form tied into our ticketing system. Before access is granted, the system owner and/or department manager must approve the request.

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 vendors Access Control Policy dictates all access is to be assigned on least privilege basis. All access requests require management approval in the vendors ticketing system.

Permission based access policy is used: In regards to Member PII data:
1-Lifecare employees must first log into our system with their network credentials.
2-Roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. The vendor staff are assigned particular roles tied to their job function, and through those role assignments acquire the computer permissions to perform particular computer-system functions or access data. Users are not assigned permissions directly, but only acquire them through their role (or 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.

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 Systems Security Awareness
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 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 File (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 within the organization is supported by a series of physical, 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. Within the specific applications each user is give a secured account ID and is assigned to the appropriate role(s) and permission list(s) based on their job functions.

Technical Security - The user is allowed three attempts to login correctly prior to being locked-out of the workstation. After 15 minutes of inactivity the workstation is locked and requires the user to re-authenticate prior to re-establishing access to any applications. Users are required to change their passwords every 90 days. The Web site leverages 256-bit Secure Socket Layer (SSL) encryption. Users of the website create their own user ID and passwords upon their initial visit to the site. Passwords are entered into non-display fields.

Physical Security - The office suite entrance doors are secure; requiring each employee to present their assigned security cardkey for access. The main building facility doors are open during normal visiting hours to allow entry and are secured during non-business hours, requiring the secured cardkey access. The building and parking areas are patrolled by security personnel.

Identify the publicly-available URL:

The current URL is:

https://www.worklife4you.com/index.html

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?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

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?

Yes

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

Yes