US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/03/2016

OPDIV:

OS

Name:

Online Medical Evaluation Tool

PIA Unique Identifier:

P-5216119-967309

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.

Contractor

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.

There have been no changes since the last review PIA.

Describe the purpose of the system.

The purpose of Online Medical Evaluation's (OME) is to provide a web-based medical evaluation system for determining whether or not federal employees who may need to wear respiratory protection as a part of their job are medically qualified to do so.

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

The system collects information from federal employees for the purpose of completing medical questionnaire evaluations required before the employees can wear respiratory protection as a part of their employment. The OME process begins with the Operating Division providing the applicable employees the Occupational Safety and Health Administration (OSHA) Respirator Medical Evaluation Questionnaire to complete online. These employees are receiving this questionnaire to

determine their need/ability to wear respiratory protection because ones work environment could prompt the need for this protection. The agency administrator notifies their employees via email when they want them to take the evaluation and provides a secure link to do so. The system collects information about individuals including name, employee ID numbers, date of birth, email address, responses to questionnaires and medical notes about health status and conditions (no medical examinations are conducted), and determinations about the employees' ability to wear a respirator as part of their professional duties as employees. The email addresses of those completing the questionnaire are also collected because OSHA requires that employees taking the questionnaire are notified of their evaluation outcome. The information collected from employees is accessible only to authorized medical personnel (agency doctors and nurses and OME doctors). The doctors and nurses log into a secure doctor or nurse specific URL to view the information they need to determine whether an employee can safely wear a respirator. The evaluation results are sent via a system generated encrypted email message telling the employee whether they are certified to wear a respirator or not.

Doctors, nurses and administrators accounts must be pre-approved by the Federal Occupational Health (FOH) Contracting Officer's Representative (COR). Once approved, the vendor is provided the account form to set up their system access. Their email address, password and their security question and answer are a part of their user credentials. Their password and security question and answer are stored as non reversible encryption. The email address of the FOH Doctors, nurses and administrators are used as a part of their credentials. The vendor doctors use their professional email address as a part of their credentials in order to access the system.
There are federal Agencies outside of HHS that use this system. The only personal information shared with the appropriate agency administrators or any other non-medical personnel consists of employee names and ID numbers, which are needed to manage participation in the program. Those agencies include Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), Federal Protective Services (FPS), United States Postal Service (USPS), Transportation Security Administration (TSA), Federal Air Marshall Service (FAMS), Social Security Administration (SSA), United States Department of Agriculture (USDA), National Transportation Safety Board (NTSB), Federal Aviation Administration (FAA), Department of Interior (DOI), National Park Service (NPS), USMINT and Federal Emergency Management Agency (FEMA).

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

The system collects information from federal employees for the purpose of completing medical questionnaire evaluations required before the employees can wear respiratory protection as a part of their employment. The OME process begins with the Operating Division providing the applicable employees the Occupational Safety and Health Administration (OSHA) Respirator Medical Evaluation Questionnaire to complete online. These employees are receiving this questionnaire to determine their need/ability to wear respiratory protection because ones work environment could prompt the need for this protection. The agency administrator notifies their employees via email when they want them to take the evaluation and provides a secure link to do so. The system collects information about individuals including name, employee ID numbers, responses to questionnaires about health status and conditions (no medical examinations are conducted), and determinations about the employees' ability to wear a respirator as part of their professional duties as employees. The email addresses of those completing the questionnaire are also collected because OSHA requires that employees taking the questionnaire are notified of their evaluation outcome. The information collected from employees is accessible only to authorized medical personnel (agency doctors and nurses and OME doctors). The doctors and nurses log into a secure doctor or nurse specific URL to view the information they need to determine whether an employee can safely wear a respirator. The evaluation results are sent via a system generated encrypted email message telling

the employee whether they are certified to wear a respirator or not.

Doctors, nurses and administrators must be pre-approved by the Federal Occupational Health (FOH) Contracting Officer's Representative (COR) and the vendor in order to receive credentials to access the system. Once approved, their email address, password and their security question and answer are a part of their user credentials. Their password and security question and answer are stored as non reversible encryption.
There are federal Agencies outside of HHS that use this system. The only personal information shared with the appropriate agency administrators or any other non-medical personnel consists of employee names and ID numbers, which are needed to manage participation in the program. Those agencies include: CBP, ICE,FPS, USPS, TSA, FAMS, SSA,USDA, NTSB, FAA, DOI, USMINT and FEMA

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

Medical Notes

Responses to a medical questionnaire on health status, decision on whether the individual may use

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

Employees

Vendor/Suppliers/Contractors

None

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

The primary purpose of the personally identifiable information (PII) used is work e-mail addresses to identify administrators and provide information to administrators and employees. As well as, names and designated ID numbers of employees are used by system administrators to manage respiratory protection programs.

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

A report can be generated that would show the employee name and their unique ID number. This report would be used to determine if the employee passed or failed their need for a respirator. The administrator supervisors would generate and review this report.

PII is not disseminated to anyone, including the employees themselves, without a “Release of Medical Information" consent from the employee. When consent is granted, the information may be released to the employee or directly to a medical provider if authorized by the employee. There is an Employee Medical File System Manager within each agency that tracks the release of medical information requests. Medical information is sent if necessary either via secure fax or certified mail.

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.

OPM/GOVT-10 Employee Medical File System

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

This program does not collect information 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

Within HHS, the only personal information shared with the appropriate agency administrators or any other non-medical personnel consists of employee names and ID numbers, which are needed to manage participation in the program.

Other Federal Agencies

Other Federal Agencies that have this system, the only personal information shared with the appropriate agency administrators or any other non-medical personnel consists of employee names and ID numbers, which are needed to manage participation in the program.
Those agencies include: CBP, ICE, FPS, USPS, TSA, FAMS, SSA,USDA, NTSB, FAA, DOI, USMINT and FEMA

Private Sector

Employees that complete a "Release of Medical Information" consent form may receive information directly or information can be provided directly to a medical provider if the request has been authorized by the employee. This may occur for different reasons such as, but not limited to: an employee can not definitively answer the questions within the OME system as it pertains to their health as the respirator relates to their job duties due to other health concerns that employee may have.

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

Agencies that elect FOH services complete an inter-agency agreement. This agreement allows agencies to offer the applicable FOH services to their personnel per the agreement terms and conditions. The agreement will contain the FOH services that a particular agency decides to offer to its staff. For example: a facility gym, medical staff on-site. In addition, the agreement authorizes information sharing and disclosure.

Describe the procedures for accounting for disclosures.

PII is not disseminated to anyone, including the employees themselves, without a “Release of Medical Information" consent from the employee. When consent is granted, the information may be released to the employee or directly to a medical provider if authorized by the employee. At each agency there is an Employee Medical File System Manager that manages the employee file including the Release of Medical Information. The manager tracks the releases via a spreadsheet.

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 notified that their personal information will be collected via the "OME Privacy Policy Notice". The notice states that no PII about the actual individual is collected unless they choose to provide that information.

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.

Submission of PII is voluntary, but required before assuming duties that require wearing a respirator. Employees are given the choice to opt out of completing the online questionnaire. Before the questionnaire begins, employees are informed of the purpose which is to protect them from potential hazards in their work environment and reduce exposure to harmful agents. In addition, non-participation is explained, this can affect ones ability to enter certain work environments and may result in disciplinary action for failure to follow instructions. At that point, employees may select a button that they disagree with the process which opts them out of the questionnaire. If they select the agree button, they will continue with the questionnaire process. If the employee begins the questionnaire and decides not to continue, they can just close the browser.

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

No major changes have occurred to this system to date. However, in the event that a major change was required, the contractor owned contractor operated vendor would work with the FOH OME Contracting Officer's Representative (COR) to determine how to communicate changes to the end users.

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.

Contact information is included on our website. Any such complaint would be reviewed by our Chief Operating Officer, who would involve others as deemed appropriate for addressing the concern, such as the Computer Security Incident Response Center (CSIRC) if appropriate.

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

The system owner conducts an annual security assessment of the OME system security controls the system's data integrity, availability, accuracy and relevancy are a part of this annual assessment process. The vendor maintains a fully functional backup of the production system to ensure availability. Data integrity is maintained through the encryption of the data at rest and in transit. The annual assessment of the government system security requirements checks to ensure that the vendor steps are accurate relevant to making sure that the system is compliant.

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

Users:

Users enter PII when completing questionnaires, then have no additional online access. The system is designed to collect employee input for purposes of medical evaluations. They are the only parties who can provide the information.

Administrators:

Access is limited to names and IDs of employees for whom they are responsible. Access is required for them to properly manage respiratory protection programs.

Developers:

Two people only, for purposes of assisting medical personnel to improve process flow, assist with data retrieval, or help provide records to employees upon request

Contractors:

If staffing necessitates the need, sometime contract doctors are utilized.

Others:

Medical personnel must review the data employees input in order to complete a medical evaluation. Customer Service staff assist users and administrators. (vendor medical personnel, FOH medical personnel, vendor Customer Service Staff)

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).

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 what 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 and privacy awareness materials, at least annually and prior to the employee's use of, or access to, information systems.

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.

As exerted from System of Records Notice (SORN) OPM/Gov-10, which covers current and former Federal civilian employees as defined in 5 U.S.C. 2105. Records retained included but are not limited to:

Medical records, forms, and reports completed during employment as a condition of employment, either by the employing agency or by another agency, State or local government entity, or a private sector entity under contract to the employing agency

RETENTION AND DISPOSAL:
The Employee Medical File (EMF) is maintained for the period of the employee's service in the agency and is then transferred to the National Personnel Records Center for storage, or as appropriate, to the next employing Federal agency. Other medical records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration's records schedules or destroyed when they have served their purpose or when the

employee leaves the agency. Within 90 days after the individual separates from the Federal service, the EMF is sent to the National Personnel Records Center for storage. Destruction of the EMF is in accordance with General Records Schedule-1(21). Records arising in connection with employee drug testing under Executive Order 12564 are generally retained for up to 3 years. Records are destroyed by shredding, burning, or by erasing the disk.

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.

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.