US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/16/2016

OPDIV:

OS

Name:

Staff Portal Website

PIA Unique Identifier:

P-5310976-085253

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

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

Describe the purpose of the system.

The purpose of Federal Occupational Health (FOH) Staff Portal Web Site is to deliver up-to-date information about FOH programs and activities to FOH staff. The Portal also provides specific applications that are used by staff. Examples of these applications include tracking of the completion of mandatory training such as Security Awareness Training, management of FOH equipment inventory, and providing official staff roster/management capability. The Portal also provides a mechanism to capture medical notes and contains FOH employees work and personal contact information.

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

The Portal provides a mechanism to capture project documents and calendars, medical notes shared between team members, a staff directory containing FOH employees work contact information. Within the staff directory users can perform a basic search of an employee by entering any of the following: First name, Last name, State of work location.

An advanced search can be performed as well selecting any of the following: First name, Last name, State of work location, position, staff type(civil servant, commissioned corps, contractor), Occupational Health division, Occupational Health Team. The information that can display is the employees first name, last name, work position title, work phone number, work cell phone number if applicable, fax number if applicable, work email address, alternate work locations if applicable, Manager, Contract Vendor company name (if a contractor) staff type (civil servant, commissioned corps or contractor) work certifications, and other proprietary information such as: security assessment documentation from vendors and process and procedure information related to clinical policies required for The Joint Commission (TJC) accreditation.

TJC is an independent non-profit organization that accredits and certifies health care organizations. Policies developed as a part of the TJC accreditation process are stored on this site. These are general process documents that explain how Occupational Health performed certain tasks. Occupational Health Contractor owned contractor operated (COCO) vendors submit their security documentation drafts for review in preparation of their security control assessments. Medical notes are reviewed when necessary. The medical notes in the system include a reference number that matches to the customer's system (specifically for workman's comp claims from Department of Labor (DOL). DOL has a number in their system that Occupational Health clinicians reference in the notes so that all can keep track.

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

The Staff Portal Web Site (Staff Portal) is an employee collaboration resource. The Staff Portal is organized into 4 primary areas:

Home Page: Provides a vehicle for organizational communications for FOH staff.

Division Section: Provides basic information about major FOH business units. Information that the Division wants users to be aware of if needed, for example, The Clinical Health page contains information regarding Ebola. In addition to information about various health screenings, each divisions pages are developed based on that particular division.

Projects and Teams: Collaboration sites broken down by initiative, workgroup, or project team. Depending on staff roles and responsibilities, users can access medical notes of patients and the medical record number could appear within that documentation along with the patients contact information: Name, mailing address, date of birth, phone number, military status if applicable, employment status (if provided), email address (if provided) and biometric data(height and weight).

Shared Services: Information and employee self-service, such as for computer assistance, general information such as how to report a security incident, Health Insurance Portability and Accountability Act (HIPAA) and PII policies, marketing materials and templates, IT training, office locations, reporting system issues and PSC and HHS policies. In addition to The Official Staff and Information Registry Index System (OSIRIS) which is a central repository database system designed to help users manage staff listings, contact information, phone numbers, records and FOH software applications. OSIRIS contains Federal employee and contractors name, email address, phone number and work location.

Federal employees and contractors that have access to the system can login with their HHS network login credentials. Contractor owned contractor operated (COCO) vendors have a user ID assigned and they are provided with their initial password to login to the system the first time. Federal Employees and direct contractors that require access to the staff portal must have their manager contact the FOH help desk and state the required user access role on the site. These users will access the site with their HHS credentials which will direct them to the specific pages as determined by their manager.

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

Biometric Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Certificates

Education Records

Military Status

Employment Status

HHS User Credentials

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

Employees

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

FOH Federal employees, their contractors and some of their vendors have the applicable permissions to place documents on the portal for others that have access to that particular page for viewing. The PII is primarily used on this site for awareness of those entering information into the site for record keeping purposes.

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?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Online

Government Sources

Within OpDiv

Other Federal Entities

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?

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.

On the login screen for this system as part of the Terms of Use that appears on the login page it states "You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system. Any communication or data transiting or stored on this information system may be disclosed orused for any lawful Government purpose."

After accessing the system, individuals will see their name next to the document they have uploaded into the system. They are placing this information onto the site because they want to share that document with others to view.

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 way for a person to opt out of their name appearing next to the document that they've uploaded onto the staff portal unless they don't upload the document at all or they send a secure encrypted zip file of the document to whomever they want to have access to that particular information.

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

Email notifications would be distributed to those users that have active credentials within the system regarding any major changes that would be occurring to the system.

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 contact the FOH helpdesk in the event that they have any issues with the system.

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 Staff Portal website is a minor system under the FOH Communication System. 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.

Regarding the review of the accuracy and relevancy of the PII, the user is responsible for ensuring that the data is accurate and relevant. Any name change updates need to be communicated to the FOH helpdesk.

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

Users:

Clinical staff that needs to review a patient's medical records as a part of their job duties. Security staff that needs to view contractor/vendor security documentation drafts.

Administrators:

Administrators who have a need-to-know the users name, email address and phone number when setting up their system permissions and adding and modifying staff information in OSIRIS if necessary.

Contractors:

COCO vendors may provide PII information when providing drafts of their information security documentation for review.

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. Individuals are assigned access to pages on the portal based on their role. If a user works in Clinical and needs to review patient medical records based on their job functions then they will be granted to the particular client url within the portal to see that particular clients medical records. Users are assigned access to the portal by their manager based on their job roles and responsibilities. Users are only assigned access to the specific areas of the portal needed to perform their job.

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 systems have the capability to share different components of the systems with different personnel based on need. There are multiple roles that can be assigned or not assigned as appropriate for their system usage.

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 members (employees and contractors) to be exposed to security awareness materials, at least annually and prior to the members 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).

Staff members 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 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.

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.