US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/01/2016

OPDIV:

OS

Name:

FedHealth System

PIA Unique Identifier:

P-8723145-553606

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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.

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.

FedHealth is an occupational health and safety management system used to support the business needs of Federal Occupational Health (FOH), a division of HHS Program Support Center (PSC). These needs include providing medical examinations and case reviews for FOH's medical work clearance and surveillance program. This program provides these services for civil federal employees whose job requires that they meet specific medical requirements in order to perform their job safely. For example, weapons carriers, park rangers, animal handlers, and other jobs that might put a worker at risk of being exposed to chemical/toxic substances require medical work exams to monitor their ongoing health and to monitor any potential exposures to harmful substances. FedHealth also support case review management for FOH's medical employability program which provides case review support for reasonable accommodation, fit-for-duty, family medical leave act requests, and occupational worker's compensation cases. The system provides an electronic health record functionality to collect and document medical test results for employees enrolled in the medical clearance and surveillance program.

FedHealth also contains functionality to process customer/agency agreements and fudning sources for those agencies wishing to purchase such services from FOH. This service and charge management functionality provides the ability to generate service orders for all types of FOH services including their wellness, fitness and health promotion programs, environmental health, safety and training program and the behavioral health program which provides employee assistance and work life services to subscribing federal agencies.
FedHealth contains case management functionality for behavioral health cases which use a separate person/case record than the one created for a person's medical examination records.
In addition, the system provides the ability for authorized agency occupational health and safety managers to access the status of their employee's medical work clearances. FedHealth also provides the employees who require medical work clearances with the ability to complete their pre-examination appointment medical forms on-line.

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

The FedHealth system will store customer agreement, statement of work, funding source data as well as agency contact information, clinical health data for medical clearance and surveillance examinations as well as walk-in health services. The system will also store medical case information for medical employability case reviews for reasonable accommodation, disability reviews and family medical leave act (FMLA) case types. Also,the agency employee's work address, last 4 digits of their SSN which are hidden, date of birth, gender, race and ethnicity (optional) , job title and supervisor POC are maintained within FedHealth.

The service and charge management functionality contains customer agency name, address information and the associated agency contact data for agency financial points of contact (POC), occupational health and safety management staff and supervisor contact information for those responsible for medical work clearances for their employees. Funding source information is maintained within FedHealth which is used to pay for charges for services rendered. Requests for services by customers is maintained as a service order within the system and those external, authorized service providers are maintained within the system in order to receive service referrals.

The medical work clearance and surveillance functionality collects medical work history and medical testing data for those customer agency employees requiring medical work examinations. Medical testing data include results of EKG's, chest XRAYS, audiograms, spirometry, vision testing , laboratory tests, physician examination and vaccination history. The system tracks services for wellness screenings, flu vaccinations and health promotion services.

The Medical Employability Program maintains data provided by the customer/agency employee in support of their reasonable accommodation, family medical leave act, disability review and other related case types. FOH Reviewing Medical Officers (RMO's) store case notes and their medical opinion within the system.

The Behavioral Health case management functionality maintains a physically separate person record for those employees able to access this service. Personal medical records and behavioral health records are stored in different partitions and are completely distinct from each other. The behavioral health person record maintains information about the date/time of the call from the employee, the case type, presenting issue/chief complaint, and their demographics in order to refer them to a counselor.

User credentials are stored via Access Management System (AMS) and therefore, are not stored in the FedHealth system. The user credentials in AMS includes name, email address (HHS email addresses), PIV card badge number, agency name.

NOTE: All agency employees using the medical employability and medical clearance/surveillance program services sign an Authorization for Disclosure form and are provided the Privacy Act notice.

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

The agency employee's work address, last 4 digits of their SSN which are hidden, date of birth, gender, race and ethnicity (optional) , job title and supervisor POC are maintained within FedHealth. User credentials are stored via AMS and therefore, are not stored in the FedHealth system. The user credentials in AMS includes name, email address, PIV card badge number, agency name. Email address is also maintained which allows FedHealth to send electronic appointment confirmations, reminders and cancellation notices. Each agency employee is then associated with one or more medical panels which is the list of examination services required for medical testing which depends upon the agency medical standards document and their job. Medical panels are created in FedHealth to include frequency of examination for agency employees depending upon age range and gender. Laboratory testing requires the employee's date of birth for analysis purposes. For some cases, FOH will refer the examination to an external Private Provider Network (PPN) which is operated by a contractor directed to perform such medical examinations for those agency employees that do not live or work near a FOH operated health clinic.

The referral request is sent to the PPN with an electronic packet of forms to use in performing and documenting the test results. Each page of the e-packet is bar-coded in order to minimize exposure to Personally Identifiable Information (PII). For example, the bar code stores an encrypted chart ID, encounter ID data items in order to use when matching the incoming e-packet with the referral stored within FedHealth. The bar code eliminates the need to expose any person data items not directly required by the examining service provider. The date of birth is required due to the needs of the laboratory testing (when applicable), however, the agency name, full name, gender etc are not required to be shared. The authorized POC for the Medical Employability Program is usually a member of the agency's Human resource or Equal Employment Opportunity Commission (EEOC) department. As with the medical work clearance program, these individuals must be listed as an authorized person on the agency's agreement for the program. FedHealth will only allow access to designated case medical opinions that are authorized within the system and approved by the agency. Supporting data for both programs may be sent to FedHealth's secure fax server which is located within the secure data center. Incoming data sets/pages are consumed via the fax server and matched to the appropriate case. Medical opinions for cases are made available to authorized agency POC's in a secure manner when they access their agency portal.

All individuals must have a valid Homeland Security Presidential Directive (HSPD)-12 Personal Identity Verification (PIV) card and must be registered with the HHS Access Management System (AMS) for single sign-on to their authorized access to FedHealth. This includes all FOH end-users including clinicians working at a FOH operated clinic and/or an external service provider. FedHealth also provides appointment management support via the FedHealth Customer Care Center (CCC) which will be located in PSC's operations center in Salt Lake City, Utah. This CCC will schedule examination appointments in support of FOH's medical employability and medical clearance/ surveillance program services. These individuals will assist agency employees with completing their on-line pre-appointment forms and questionnaires and will work with FOH's enrollment managers to insure that the examination appointments are scheduled, performed and completed in the required time frame. The Behavioral Health case management functionality shares only limited information if made available with the affiliate service provider in order to limit and/or eliminate the need for exposure of PII.

NOTE: Agency employees accessing behavioral health and work life services may do so anonym

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Employment Status

Last 4 of SSN is collected, race and ethnicity is optional,chart ID, and encounter ID data items

Medical testing results for vitals, hearing testing, vision testing, lab results for comprehensive blood profile, chest x-ray results, medical history data, EKG results
Supporting documents for medical case reviews such as parking permits, reasonable accommodations, family medical leave act, disability reviews
Vaccination records, wellness and screenings data, physical exam reviews and physician notes

Agency supervisor information, job title/role, case review notes, behavioral health case descriptions excluding personal case details that are private between the counselor and the employee

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

Employees

Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Identification when entering a health clinic, exam component determination based upon a patient's age, communications regarding medical clearance and surveillance programs.
PII ad Protected Health Information (PHI) is required in providing case review services for FOH's medical employability program which support case requests for reasonable accommodation, family medical leave act, disability reviews and handicap parking permit requests.

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

The Environmental Health and Safety division of FOH provides mandatory Environmental Health training courses for some agencies per their request. The employees SSN is collected in order for the requesting agency to match the training records with their own internal database. This training program is used rarely and only by the Architect of the Capital agency.

Describe the function of the SSN.

The last 4 digits of a person's social security number are collected as a form of identification which is used in conjunction with other data elements. Some agencies request that FOH collect the entire SSN for matching with their own internal databases as the medical charts maintained within FedHealth are the property of the agency. FOH is the custodian of the data.
The full or partial SSN is always hidden on the screen and encrypted within the database. It is not a mandatory field.

When an employee checks in a clinic for their examination appointment, the check-in procedures state that the nurse must confirm identification by asking several questions of the employee standing in front of them. The last 4 digits of their SSN may be one of the questions along with other data items.

Cite the legal authority to use the SSN.

Federal Occupational Health employee health record data is protected by The Privacy Act of 1974 (5 U.S.C. §522a), Genetic Information Nondiscrimination Act of 2008, 42 CFR Part 2, and subject to regulations within 5 CFR §§ 293 and 297, CFR 1910.1020, 44 U.S.C. §§3541-49, 29 U.S.C. §§657 and The National Archives and Records Administration (NARA) General Records Schedules (GRS)

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

Federal Occupational Health employee health record data is protected by the Genetic Information Nondiscrimination Act of 2008, 42 CFR Part 2, and subject to regulations within 5 CFR §§ 293 and 297, CFR 1910.1020, 44 U.S.C. §§3541-49, 29 U.S.C. §§657.

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 Records

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

Identify the OMB information collection approval number and expiration date

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.

The current and standard policy is to provide the Privacy Act Notice to employee patients and to obtain a signed release and disclosure form when services are provided in the health clinics as well as when provided Medical Employability services. The FedHealth will use the same policy and practices but will collect the signature electronically and will make the Privacy Act Notice more accessible both in written and electronic format.

For those employees whose job requires a medical work clearance and/or has submitted a medical employability case request, the authorization for disclosure is required. If the employee refuses to sign the authorization, the case review cannot be performed. In some cases, the agency may require this as part of the job requirements making the employee ineligible for the position.
There are some exam types (i..e wellness exam services) that are voluntary and are provided as a courtesy from the agency to their employees. For these exam types, the exam is voluntary and the employee must sign the authorization for disclosure as part of the voluntary exam service.

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.

Individuals will not be allowed to opt-out of the collection or use of their PII, as it is required to effectively store medical information.

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

Because FOH is the custodian of the data, the agency (actual owner of the data) shall be notified in writing by FOH in the event when major changes to the system occur. For planned major changes, the notification shall be sent at least 30 days prior to the change date. Agency recipients include those agency individuals who are listed as contacts on the agency agreement.

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 FedHealth IT Configuration team will follow HHS Security Policies and all data breaches or security incidents will be reported to HHS Computer Security Incident Response Center (CSIRC) for remediation.

FedHealth will allow users to submit an incident report via email or phone to the Customer Care Center (CCC) in the event they are informed of any inappropriate disclosure or use of their PII. Upon notification of such an incident, the CCC will immediately contact the Security Incident Response Team (SIRT), who will launch an investigation to verify the incident and identify any potential risks to the system or the data contained within it. The CCC will also immediately notify FOH management of the incident, and keep senior personnel apprised of the situation as it develops.

In the event an individual notices inaccurate PII within the system, they will be able to contact the CCC via email or phone. The CCC will then notify FedHealth systems administrators with the appropriate access, who will be responsible for the identification and resolution of the inaccurate information, as well as investigating the circumstances surrounding the inaccuracy. In the event the system administrator identified a potential breach or risk to the system, they will initiate the FedHealth Incident Response Plan, and notify the SIRT and FOH management.

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

FedHealth's electronic background process is capable of monitoring, logging, and reporting software activity by each user account or network device. This capability will detect unauthorized accesses and changes to information. The system reviews can be conducted through using the system reports.

All changes to data are stored for audit and historical purposes. Additionally, security access control rights/roles are created to limit the FOH positions that have the authority to update PII data. Standard operating procedures are being developed to permit the updating of PII by authorized FOH individuals. For example, if the employee requests that their last name be changed due to marriage, they must provide FOH will a copy of their marriage certificate. A copy of such documentation shall be stored with the employee record within FedHealth. Additionally, the agency POC shall be included as part of the notification/approval process which is electronically routed and tracked. Nurses in the clinics will not have the authority to change PII. Rather, they will notify the employee requesting the change of the standard operating procedure and process.

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

Users:

Nurses and physicians in FOH health clinics are required to collected this information as a part of their medical record. Medical clearance program Enrollment Managers will work with the agency POC's to create employee records and to enroll such individuals into the appropriate medical panel for testing purposes.

Administrators:

As system administrators, they will have access to data but will not have a need to know unless an issue arises and needs troubleshooting. Access will be recorded and audited.

Contractors:

Direct HHS contractors accessing the system and performing work for FOH include nurses, physicians, reviewing medical officers (physicians) and enrollment managers. These individuals currently have access to such data.

Others:

FOH Customer Call Center specialists will have minimal access to the PII data in order to support employees and end-users.

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

All end-user accounts will be managed by the FedHealth IT Configuration team within FOH. Customers may submit requests for access to their FOH Account Executive who will work with the FOH FedHealth IT Configuration team to accommodate such requests. An online form will be made available to customers which will include the proper approvals for granting access to employees within an agency. Only specific positions and roles within FOH are allowed access to PII and PHI. Background clearances are standard with the provision of such data access.

Authorized individuals (supervisors) of requesting end-user accounts must approve access to FedHealth based upon the role requested. Each potential end-user of FedHealth must attend application and FedHealth security training prior to being approved for a FedHealth end-user account. Ongoing FedHealth security and application training is provided and will be mandatory for all end-user groups, especially those that may have access to PII and PHI.

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.

FedHealth is capable of restricting end-user's access by organization, functional module, and objects within a module. FOH FedHealth IT Configuration team will work with FOH Account Executive to manage and control end-user's access.

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.

All system users will complete required Annual HHS Security Awareness and Privacy Awareness Training.

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

Users will receive training on Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the FedHealth System Training. Users working with customer employee records will be training on identification validation practices within the clinical setting.

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.

PII data will not be deleted or purged from the system. All inactive information will be flagged with In-active Status.

NARA GRS-1 is the retention schedule for the FedHealth system.

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

1. PII and PHI is maintained and secured administratively through the implementation and enforcement of standard operating procedures in conjunction with technical access control rights and business rules defined within the system.

2. Security access rights are created at the data element level by data set in addition to row-level access control. These roles are granted only to authorized end-users within the system on a need to know basis.

3. Administrative business processes and approval cycles have been implemented within the system for only key individuals to update and secure such data in the system.

4. All users accessing PII and PHI are required to access the system with their HSPD-12 PIV card.
5. The system does not allow printing or downloading of medical chart data.
6. The system does not allow screen prints of the system to be taken.
7. The system will notify FedHealth IT management when PII and/or PHI is accessed by individuals outside of normal working hours.
8. The data center is rated to support systems with high security ratings.
9. Access to all data sets and PII and PHI in particular are audited and changes tracked and recorded 24x7.
10. Such audit logs are scanned and monitored for unusual behavior.
11. Security controls have been implemented at the physical hardware, network, database levels and application to secure PII and PHI per the System Security Plan - Appendix X document.
12. Database is encrypted at rest and in-transit to protect sensitive PII and PHI data.