US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/14/2016

OPDIV:

OS

Name:

Private Provider Network Client Portal System

PIA Unique Identifier:

P-6382246-308232

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?

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 Private Provider Network Client Portal (PPN-CP) contains exam scheduling and tracking for Federal Occupational Health (FOH) medical examinations. Federal employee's examinations are scheduled via PPN-CP when a Federal Occupational Health Unit does not exist in their city/state. FOH users access PPN-CP with a username and password, and populate referrals for examination requests when necessary, also referred to as “cases” in the PPN-CP system. The FOH users can attach the relevant medical records to referrals. Once the information is in PPN-CP, the vendor finds a medical provider in the applicable service area to perform the medical examination based on the referral and schedules the appointment. Once the appointment is scheduled, the provider receives the patient's medical information via secured FAX. Providers cannot access PPN-CP. The exam results are sent back to PPN-CP via secure FAX and are automatically loaded into the system. The vendor is alerted when the exam results are loaded. The results are reviewed by the vendor for accuracy.

FOH personnel can access PPN-CP to check on the status of the exam. Ex. the date of the appointment and whether the exam has been completed or not. Once the results have been reviewed for accuracy by the vendor, the vendor sends the examination to the Agreement Manager Assistant (AMA) via United Parcel Service (UPS). The examination is reviewed by the Reviewing Medical Officer who determines whether the employee is medically qualified or not to perform their job tasks. A determination letter is sent to the agency that requested the examination and the employee. The letter states whether the employee is medically qualified or not to perform their job tasks. The roles of the FOH users that may access Personally Identifiable Information (PII) information are: Service Delivery Lead, Operations Lead, Data Entry Clerk, Administrative Assistant, and Physician. PII is accessed by authorized vendor case coordinators (exam schedulers and those reviewing medical records for accuracy), as well as, examining Providers to complete the examination process. No other entity is authorized to view or handle the data.

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

The system collects information about FOH employees including PII as described; Full name, Maiden Name, Social Security Number, Taxpayer Identification Number, Street Address, Mailing Address, Email Address, Date of Birth, Phone Numbers, Medical Notes, Medical Record Number, Employment Status, Certificates, Military Status, Service Information, Medical Information.

The system collects information from federal employees for the purpose of occupational health examinations and counseling as part of their employment.

PPN-CP collects the following information regarding its system users including system administrators: user name, name (last, first, middle), work phone, fax number, primary job title, email including an hhs.gov email if provided (the hhs.gov email can be from FOH Federal employees or direct contractors), employee state (as in CA, VA, FL etc), created date, created user (user who created the user), modified date and modified user (user who modified the user)

Card readers at the external entries of the systems data center facility. Biometric hand scanners are used inconjunction with the card reader in order to obtain access.

The National Guard personnel included within this process are civilian and military employees. National Guard recruits are not included. The system information listed above is collected for the National Guard personnel in order to schedule and provide medical exams for them.

The roles of the FOH users that may access PII are: Service Delivery Lead, Operations Lead, Data Entry Clerk, Administrative Assistant, and Physician. PII is accessed by authorized vendor case coordinators (exam schedulers and those reviewing medical records for accuracy), as well as, examining Providers to complete the examination process. No other entity is authorized to view or handle the data.

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

PPN-CP collects the following information regarding its system users including system administrators: user name, name (last, first, middle), work phone, fax number, primary job title, email including an hhs.gov email if provided (the hhs.gov email can be from FOH Federal employees or direct contractors), employee state (as in CA, VA, FL etc), created date, created user (user who created the user), modified date and modified user (user who modified the user)

Card readers at the external entries of the systems data center facility. Biometric hand scanners are used inconjunction with the card reader in order to obtain access.

The request for examinations is provided by FOH. FOH users access PPN-CP with their username and password and populate referrals for examination requests when necessary, also referred to as “cases” in the PPN-CP system. The FOH users attach the relevant medical records to each referral.

Once the information is in PPN-CP, vendor personnel find a medical provider in the applicable service area to perform the medical examination based on the referral and schedules the appointment. Once the appointment is scheduled, the provider receives the patients medical information via secured FAX. Providers cannot access PPN-CP. The exam results are sent back to PPN-CP via secure FAX and are automatically loaded into the system. Vendor personnel is alerted when the exam results are loaded. The results are reviewed by the vendor for accuracy. FOH personnel can access PPN-CP to check on the status of the exam. Ex. the date of the appointment and whether the exam has been completed or not. Once the results have been reviewed for accuracy by the vendor, the vendor sends the examination to the Agreement Manager Assistant (AMA) via UPS. The examination is reviewed by the Reviewing Medical Officer who determines whether the employee is medically qualified or not to perform their job tasks. A determination letter is sent to the agency that requested the examination and the employee. The letter states whether the employee is medically qualified or not to perform their job tasks.

For National Guard examinations, the request for an examination is retrieved by FOH administrative assistant from the National Guard's MedChart system. The National Guard submits: First Name, Last Name, Email Address, Date of Birth, Sex, Comments (including exam type), Supervisors name and supervisors phone number. In addition, the following items that maybe collected include: an exam id, exam request type (whether exam is requested or canceled), last 4 digits of Social Security Number, Preferred Exam City, Preferred Exam State, Preferred Exam Zip code. This information is retrieved from the MedChart system daily when necessary. This information is uploaded into PPN-CP by the FOH administrative assistant. The FOH administrative assistant retrieves the following information daily when necessary from PPN-CP: Exam ID, status date, Date filed in PPN-CP, Appointment Date and Appointment time. Once the examination is complete and the vendor personnel has reviewed the results for accuracy, the FOH administrative assistant provides the physical examinations to the Reviewing Medical Officer (RMO) for review.

The physical examination is entered into the National Guard MedChart system by the FOH data entry clerk until a determination is made by the RMO after reviewing the examination. The determination will indicate whether the person is medically qualified, medically qualified with restrictions or medically not qualified. The determination letter is attached to the physical examination in the MedChart system. The original examination is mailed to the employer point of contact and the employee via UPS.

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

Biometric Identifiers

Mother's Maiden Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Certificates

Military Status

Employment Status

Taxpayer ID

Medical information

Service Information

Username and password

Primary job title

Primary job title

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

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

PPN-CP allows the exchange of medical information between the vendor and FOH, and between the vendor and its network of providers. PII is accessed by authorized vendor case coordinators (exam schedulers and those reviewing medical records for accuracy), as well as, examining Providers to complete the examination process. No other entity is authorized to view or handle the data.

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

There are no secondary uses.

Describe the function of the SSN.

To uniquely identify service recipients and allow their records to be properly connected with their employee medical files in the agencies they work for.

Cite the legal authority to use the SSN.

FOH does not collect Social Security Number on all records, but when necessary, they do. FOH serves over 300 federal agencies. Some law enforcement and Department of Homeland Security agencies track their employee records by social security number (SSN). Since FOH provides services to some of these agencies, they are required to collect and track SSN on the employee medical records for these staff so that the customer agency can properly link these records back to the employee medical file.

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. FOH performs those services for those agency heads.

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. 5 U.S.C. 2105 defines authority to collect and maintain employee medical files.

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Online

Government Sources

Within 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

The FOH Agreement Manager (AM) and the FOH Agreement Manager Assistant (AMA) can receive examination requests from an agency and provide the examination referral to the vendor. The FOH Administrative assistant receives the examination requests from the National Guard and loads this information into PPN-CP. The FOH Data Entry Clerk enters the physical examination into the National Guard system. The Reviewing Medical Officer (physician) regardless of the employees agency reviews the examination and makes the determination whether the individual is medically qualified, medically qualified with restrictions or medically not qualified. The FOH Administrative assistant that handles the National Guard requests mails the determination letter to the National Guard point of contact and the employee. The Operations Lead reviews examinations in the event that there is a delay an examination. The FOH Agreement Manager Assistant sends the determination letter to the Agency and the employee.

Other Federal Agencies

An agency's Occupational Health Program Manager receives the determination letter informing them whether an employee is medically qualified to perform their job tasks or not. The agencies include: Bureau of Safety and Environmental Enforcement, Bureau of Reclamation, Bureau of Land Management and the Bureau of Alcohol, Tobacco, Firearms and Explosives.

Private Sector

Direct Contractors that have access to PPN-CP can download examination reports which will contain PII. Employees that have taken the examinations will receive a determination letter informing them whether they are medically qualified to perform their job tasks or not.

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

Each customer agreement has an individual inter-agency agreement with FOH. These agreements specify the services provided between FOH and its customer agency. FOH monitors these agreements to ensure that they are fulfilled and that the serviced are billed for appropriately.

Describe the procedures for accounting for disclosures.

Upon completion, the AMA inputs this information into FOH's Service Tracking and Management System (STM). STM is covered by another Privacy Impact Assessment. FOH has interagency agreements with agencies that it provides specific services. In STM, the agreements are documented including services agreed upon. There is a component within this system that tracks the work fulfilled (accomplished) and billing is generated based on the work accomplished that is reported.

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

All employees receiving care at a service provision site will be asked if they have been given a "Privacy Act Notice to Patients" (form FOH-32). This form outlines the specific purposes and routine uses for information gathered as part of performing service. Employees will be given a copy of form FOH 32 if the employee requests it. A copy of form FOH-32 will also be clearly posted at the location where employees register or present themselves for services.

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 not an opt out option. If the person declines to provide the necessary information, services are not provided since healthcare services cannot be performed without accurate information.

FOH serves over 300 agencies and some track their employment records by SSN (i.e. military and law enforcement). This system information is collected as part of the employee file and therefore FOH must collect SSN to allow those agencies to link the information to their employee record. Some agencies do not require use of SSN. Some only need a partial. We only collect what is required by the customer agency.

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

Notice of applicability of privacy act is posted in clinics and is explained by healthcare workers as needed. In some cases, the person is required to sign an acceptance of privacy act applicability, and this is kept in the exam records.

The on-line system requires all users to accept the applicability of the privacy act and records their acceptance. If a user declines, they are denied access to the system.

If there was ever a need to use data in a way not covered in the current System of Record Notice (SORN) (as defined in OPM/GOV-10 SORN), we would have to seek a privacy release from all effected people. This would be an extremely large undertaking, therefore we don't expect to change things.

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 vendor or the FOH user accessing the application would notify the FOH helpdesk within 2 hours of an actual or suspected breach of PII or protected health information(PHI) by sending an email notification to the FOH Helpdesk at FOHHelpdesk@foh.hhs.gov. The helpdesk would in turn contact the HHS incident response team within 2 hours of discovery and the Contracting Officer would be notified since this a contractor owned contractor operated system. The helpdesk and others would investigate the issue and provide a resolution.

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 has been through a security accreditation following the National Institute of Standards and Technology (NIST) 800-53 guidelines, and has been independently verified to provide data integrity and availability as required by the medial programs that use it, and on a routine basis (at least annually), it is required to demonstrate to independent auditors that these capabilities are maintained.

Data is used as part of healthcare work flow and is reviewed with the employee at the time of collection, so normal processes drive review and correction of data. While most healthcare information collected are objective measures, when exam results are collected, copies of test results (and the clearance letters) are provided to the recipient (patient), so if they have an concern about accuracy or relevance, they have an opportunity to comment on receipt of these documents and the healthcare/ program staff can amend records if it is appropriate. If there is a health issue discovered as part of the exam they will be referred to their private care provider and that physician can provide a second opinion, as well as defining and providing treatment as appropriate.

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

Users:

To perform medical referrals and deliver clinical services (such as medical reviews)

Administrators:

To administer the system

Contractors:

To deliver healthcare services

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 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 Systems 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 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 SORN OPM/Gov-10, which covers current and former Federal civilian employees as defined in 5 U.S.C. 2105.

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 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 - 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 60 days.

Physical Security - Screening access through the use of trained security personnel and/or technical means such as automated card access systems and biometric screening systems. Card readers at the external entries of the systems data center facility. Biometric hand scanners are used inconjunction with the card reader in order to obtain access.