Privacy Impact Assessment (PIA): OS - FCS - QTR2 - 2021 - OS1084870

Date Signed: 7/7/2021

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

Status:	Approved	**PIA ID:**	1341752
PIA Name:	OS - FCS - QTR2 - 2021 - OS1084870	**Title:**	OS - FOH Communications Systems
OpDiv:	OS		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	Yes
PTA - 2:	Does the system include a website or online application?	Yes
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Agency
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	Significant System Management Change
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	FOH Communication System (FCS) is moving from the Amazon Web Services (AWS) Gov Cloud to the HHS Cloud-Managed Application Hosting Center (C-MAHC).
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	**Federal Occupational Health (FOH) Communications Systems (FCS)** is an umbrella system that was designed to consolidate a

number of individual minor applications into a single MODERATE-level system security profile. No data is stored on FCS.

FCS contains 4 sub-systems:

FOH Service Tracking and Management System (FSTM)

FOH Medical Evaluation/Requirements Information Tracking System (FMERITS)

Real-Time Framework for Management (RTFM)

FedHealth

FSTM provides a complete set of tools to define the inter-agency agreements between FOH and its customer agencies, collect evidence of the fulfillment of those agreements, and provide external financial systems the information they need to bill for services rendered.
FMERITS The Medical Evaluation-Requirements Information Tracking System (FMERITS) is a system boundary hosting eight modules:

Agriculture Research Service (ARS) medical surveillance

United States Department of Agriculture (USDA-ARS)
Animal Plant Health Inspection Service (USDA-APHIS)
Medical Employability Program (MEP)
Hearing Conservation Program (HCP)

The remaining imbedded databases are included for archival purposes only:

MERITS Age Corrected Audio (HTPro)
X-Ray tracks/logs
Deployment

RTFM is a collection of tools for the centralized command and control of FCS. RTMF is responsible for Configuration Automation and Logging/Reporting. Configuration Automation is made up of code and patch repository servers. The Logging/Reporting servers provide an aggregated logging and alerting dashboard. Through centralized reporting and logging servers clear performance metrics are achieved. The logs will contain information like system reboot time, CPU usage and system events.
The information is held indefinitely.

FedHealth is an occupational health and safety management system used to support the business needs of FOH, a division of Health and Human Services (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 funding 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.

PTA - 9:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	**FCS:** There is no data stored on FCS. All sub systems store data indefinitely. **RTFM:** Real-Time Framework for Management (RTFM) is a collection of tools for the centralized

command and control of FCS.
FMERITS: All sub-systems collects and maintains Employee medical records, Name, Social Security Number (SSN), Date of Birth (DOB), gender, record IS, Agency, Address, Email address, and contact information (email address, phone number, address etc.) Other information may include height, weight, a unique identification number used in lieu if SSN, other physical characteristics, and medical information. All sub-systems retain data indefinitely.
USDA-ARS and USDA-APHIS specifically may also include physical and biological hazards.
USDA-ARS: shares information with the employee of record and employer.
Shared Information: Occupational significant findings, hearing loss. Reports to agency and employer.
USDA-APHIS: shares information with the employee of record and employer.
MEP: shares information with the employee of record and employer.
HCP: shares information with the employee of record and employer.
ATF: This is a legacy archived system but historical data is shared with the ATF organization.
Shared Information: Employment history, exposure history, duty assignment from the agency, and medical review history. ATF agents are exposed to carcinogens due to the nature of their work.
The information is shared for follow up studies on bladder cancer and other occupational issues.
HTPro, Xray and Deployment: Data is not shared, the program is no longer active.
FedHealth: 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 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. 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. 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. 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. The information is stored indefinitely.

FSTM: FSTM provides a complete set of tools to define the inter-agency agreements between FOH and its customer agencies, collect evidence of the fulfillment of those agreements, and provide external financial systems the information they need to bill for services rendered.

At this point, all data in FSTM remains indefinitely.

PII includes: name; service received; dates of birth; and an identifying number—Occupational Health recommends using the last four digits of a social security number (SSN) however, the individual can provide a different number.

HHS user credentials (user id and password) are stored in FSTM. External contract staff have an HHS user id and password assigned to them.

PTA -9A:	Are user credentials used to access the system?	Yes
PTA - 9B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Password Username
PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual	**FCS:** FCS contains no data or Personally identifiable information (PII). It acts as the umbrella server for four sub systems.

RTFM: No PII or PHI of Federal Government employees or the General Public will be stored on RTFM. RTFM will not store user names and passwords. Only the username and passwords for system administration. System administrators will only log in when changes to the configuration are required.
FMERITS: Social Security, Name, Date of Birth, Email, Phone Numbers, Medical Notes, Mailing Address, Employment Status, Employment Type, Gender, Record ID, Agency, Height, Weight, A unique identification number used in lieu of the SSN, Other physical characteristics, Medical Information, Work history, Employee and unique ID numbers. HHS Username HHS Password
FedHealth: 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. Email address is also maintained which allows FedHealth to send electronic appointment confirmations, reminders and cancellation notices. 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. 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 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. 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 anonymously.
FSTM: Much of the information in the system is non-PII, such as contractual information Other information includes financial information such as funding information for the customer agency, or authorizations to expend the funds. In a small number of cases, the agency chooses to pay using an individual's agency-issued credit card, and the credit card number may be retained. PII includes names; dates of birth; service delivered; and an identifying number—Occupational Health recommends using the last four digits of a social security number (SSN) however, the individual can provide a different number. When an employee uses an Occupational Health service which is being paid for by their agency based on the interagency agreement with Occupational Health, they are asked for this identifying number. Occupational Health recommends the last four digits of the SSN because they think users would remember that number. Individuals could conceivably decline to provide the date of birth, although in practice all of the individuals provide it. HHS user credentials (user id and password) for system administrators are also stored in FSTM. External contract staff have an HHS user id and password assigned to them.

PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	Yes
PTA - 10B:	Please specify which PII data elements are used.	**FCS**: No elements are retrieved by PII data elements **RTFM:** User name and password for admins only. **FMERITS:** Employee and unique ID numbers, HHS Username, HHS Password, Name and SSN. **FedHealth**: No elements are retrieved by PII data elements **FSTM:** Four digit identifying number that could be the last 4 digits of the Social Security Number or a random number the user selects. Name
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes
	PIA	
PIA - 1:	Indicate the type of PII that the system will collect or maintain	Social Security Number Name E-Mail Address Phone numbers Date of Birth Mailing Address Medical Records Number Employment Status User Credentials Others - RTFM: Non HHS user id and password FMERITS: Others - Agency, Employment Status, Gender Employment Type, Height, Weight, Work history and Xray. FSTM: Agency Credit Card Financial Data
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Patients Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Above 2000
PIA - 4:	For what primary purpose is the PII used?	**Federal Occupational Health (FOH) Communication System (FCS):** FCS contains no Personally Identifiable Information (PII) **FOH Service Tracking and Management**

System (FSTM): This information is used to track what tests and services have been provided to each customer and to bill appropriately. We may also aggregate this data to conduct resource planning needs.
FedHealth: Identification when entering a health clinic, exam component determination based upon a patient's age, communications regarding medical clearance and surveillance programs. Personally Identifiable Information (PII) and 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.

FOH Medical Evaluation/Requirements Information Tracking System (FMERITS): In all FMERITS sub databases personally identifiable information (PII) is described per system in the bullet list below each system primary PII use descriptions.
Medical Employability Program (MEP) :
MEP provides Federal Occupational Health (FOH) doctors with a tool to meet their surveillance goals with centralized management and reporting capabilities. FOH conducts examinations of such individuals, and the results are sent to agreement managers who direct the reports to Reviewing Medical Officers (RMO). RMOs evaluate individuals' abilities to perform their assigned tasks. Uniquely identify an individual and to be able to reference the records that apply to a specific individual.
Email address and mailing address may be used to create appointment times or deliver requested communications.
Medical information is used to deliver the requested approval or denial of the individual's physical fitness for a specific tasks/job.

Agriculture Research Service (ARS): ARS provides FOH doctors with a tool to meet their surveillance goals with centralized management and reporting capabilities. FOH conducts examinations of such individuals, and the results are sent to agreement managers who direct the reports to RMO. RMOs evaluate individuals' abilities to perform their assigned tasks. The RMO reviews occupational exposure and changes in health to confirm individuals were properly trained and protected for the work environment. Uniquely identify an individual and to be able to reference the records that apply to a specific individual. Email address and mailing address may be used to create appointment times or deliver requested communications. Medical information is used to deliver the requested approval or denial of the individual's physical fitness for a specific tasks/job.

Animal Plant Health Inspection Service (USDA-APHIS) : APHIS provides FOH doctors with a tool to meet their surveillance goals with centralized management and reporting capabilities. FOH conducts examinations of such individuals, and the results are sent to agreement managers who direct the reports to Reviewing

Medical Officers (RMO). RMOs evaluate individuals' abilities to perform their assigned tasks. The RMO reviews occupational exposure and changes in health to confirm individuals were properly trained and protected for the work environment. Uniquely identify an individual and to be able to reference the records that apply to a specific individual.
Email address and mailing address may be used to create appointment times or deliver requested communications. Medical information is used to deliver the requested approval or denial of the individual's physical fitness for a specific tasks/job.
Track exposure to work environment and the training required to protect themselves from some work environments.

Hearing Conservation Program (HCP): HCP provides FOH doctors with a tool to meet their surveillance goals with centralized management and reporting capabilities. FOH conducts examinations of such individuals, and the results are sent to agreement managers who direct the reports to Reviewing Medical Officers (RMO). RMOs evaluate individuals' abilities to perform their assigned tasks. Uniquely identify an individual and to be able to reference the records that apply to a specific individual.
Email address and mailing address may be used to create appointment times or deliver requested communications. Medical information is used to deliver the requested approval or denial of the individual's physical fitness for a specific tasks/job

Alcohol Tobacco and Firearms (ATF): ATF Reporting tool provides FOH doctors with a tool to meet their surveillance goals with centralized management and reporting capabilities. FOH conducts examinations of such individuals, and the results are sent to agreement managers who direct the reports to Reviewing Medical Officers (RMO). RMOs evaluate individuals' abilities to perform their assigned tasks. The RMO reviews occupational exposure and changes in health to confirm individuals were properly trained and protected for the work environment. Uniquely identify an individual and to be able to reference the records that apply to a specific individual.
Email address and mailing address may be used to create appointment times or deliver requested communications. Medical information is used to deliver the requested approval or denial of the individual's physical fitness for a specific tasks/job.
Track exposure to work environment and the training required to protect themselves from some work environments.

XRAY: X-Ray provides FOH doctors with a tool to meet their surveillance goals with centralized management and reporting capabilities. FOH conducts examinations of such individuals, and the results are sent to agreement managers who direct the reports to Reviewing Medical Officers (RMO). RMOs evaluate individuals' abilities to perform their assigned tasks. Uniquely identify an individual and to be able to reference the records that apply to a specific individual. Email address

		and mailing address may be used to create appointment times or deliver requested communications. Medical information is used to deliver the requested approval or denial of the individual's physical fitness for a specific tasks/job. Medical Evaluation/Requirements Information Tracking System (MERITS) Age Corrected Audio (HTPRO): The HT Pro module is an extension of the MERITS Hearing Conservation programs and allows MERITS Audiograms to be reviewed based on Occupational Safety and Health Administration (OSHA) standards for age-corrected hearing evaluations. The age-corrected audio functionality compares the new or current audiogram to the most recent baseline and provides computer-generated recommendations, based on age-corrected values, as to whether a standard threshold shift or reportable shift has occurred. The FOH RMO can then choose to accept or override the computer-suggested revisions. Uniquely identify an individual and to be able to reference the records that apply to a specific individual. Email address and mailing address may be used to create appointment times or deliver requested communications. Medical information is used to deliver the requested approval or denial of the individual's physical fitness for a specific tasks/job. Tracking of hearing ability to maintain that no hearing loss is occurring. Deployments: The Deployments sub-component within MERITS supports FOH Exam and Clearance Tracking specifically for military deployments. This application determines when an exam is needed (pre and post deployment, retirement, etc.) and tracks the clearance status. This application does not have an external interface. At this time, Deployments being used for one agency only. Uniquely identify an individual and to be able to reference the records that apply to a specific individual. Email address and mailing address may be used to create appointment times or deliver requested communications. Medical information is used to deliver the requested approval or denial of the individual's physical fitness for a specific tasks/job. **Real Time Framework for Management (RTFM):** The personally identifiable information (PII) is used for system administrators to login in to Real Time Framework for Management (RTFM). The system administrators only login when a configuration changes needs to be implemented or to run required software/security updates.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	**FCS:** FCS contains no PII

		FSTM and RTFM: The data is not used in any other capacity. **FedHealth:** The Environmental Health and Safety division of Federal Occupational Health (FOH) provides mandatory Environmental Health training courses for some agencies per their request. The employees Social Security Number (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. **FMERITS:** MEP, ARS, HCP, ATF, XRAY: Research, external reporting, and statistical analysis. USDA-APHIS, HTPRO and Deployments no second use of PII.
PIA - 6:	Describe the function of the SSN/Taxpayer ID.	**FCS:** FCS contains no PII **FSTM:** An identifying number is required of employees to assist agencies in determining if an employee has used Occupational Health Services. Occupational Health recommends using the last four digits of a social security number (SSN) however, the individual can provide a different number. This identifying number is similar to a 4 digit PIN number that agencies use to assist in identifying employees if needed that have used Occupational Health services. Occupational Health recommends the last four digits of the SSN because they think users would remember that number however, this is not required any 4 digit number can be used. **FedHealth:** 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. **FMERITS:** SSN is used in combination with name and date of birth to uniquely identify a customer agency employee. **RTFM:** N/A
PIA - 6A:	Cite the legal authority to use the SSN	**FCS:** N/A

FSTM: E.O. 12107 Rule V ""Sec. 5.2. Investigation and Evaluations. The Director may secure effective implementation of the civil service laws, rules, and regulations, and all Executive Orders (EO) imposing responsibilities on the Office by:
(a) Investigating the qualifications and suitability of applicants for positions in the competitive service. The Director may require appointments to be made subject to investigation to enable the Director to determine, after appointment, that the requirements of law or the civil service rules and regulations have been met.
The portion of the Executive Order above addresses those agencies that use Federal Occupational Health Services for applicants suitability involving a medical examination to determine if the individual can perform their duties. These are services that would be billed within Federal Occupational Health (FOH) Service Tracking and Management (FSTM).
In addition E.O. 12196 Occupational Safety and Health Programs for Federal Employees Section 1-2 Heads of Agencies states in 1-201 that the head of each agency shall: (b) The head of each agency shall: operate an occupational safety and health program in accordance with the requirements of this order and basic program elements promulgated by the Secretary.
The portion of the Executive Order above addresses the point that each agency operates an occupational safety and health program. If they use FOH services as a part of their program, they will be set up in FSTM.
The System of Records Notice (SORN) associated with this system is OPM GOVT 10 and this executive order is listed in that SORN.

FedHealth: The portion of the Executive Order above addresses those agencies that use Federal Occupational Health Services for applicants suitability involving a medical examination to determine if the individual can perform their duties. These are services that would be billed within STM.
In addition E.O. 12196 Occupational Safety and Health Programs for Federal Employees Section 1-2 Heads of Agencies states in 1-201 that the head of each agency shall: (b) The head of each agency shall: operate an occupational safety and health program in accordance with the requirements of this order and basic program elements promulgated by the Secretary.
The portion of the Executive Order above addresses the point that each agency operates an occupational safety and health program. If they use FOH services as a part of their program, they will be set up in STM.
The System of Records Notice (SORN) associated with this system is OPM GOVT 10 and this executive order is listed in that SORN.

FMERITS: Per the Privacy Act Statement, use of the Medical History and Physical Exam information is authorized by 5 U.S.C. 7901 (Health Services Programs) and 29 U.S.C. 657 (Occupational Health and Safety; Record Keeping).

RTFM: N/A

PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	**FCS:** 5 USC 301, Departmental regulations **FSTM:** 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. **FedHealth:** 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. **FMERITS:** MEP, HCP, ATF, HTPro and Deployments: Per the Privacy Act Statement, use of the Medical History and Physical Exam information is authorized by 5 U.S.C. 7901 (Health Services Programs) and 29 U.S.C. 657 (Occupational Health and Safety; Record Keeping). ARS: Authority for Maintenance of ARS: Includes the following with any revisions or amendments: Executive Orders 12107, 12196, and 12564 and 5 U.S.C. chapters 11, 31, 33, 43, 61, 63, and 83. USDA-APHIS : Authority for Maintenance of APHIS: Includes the following with any revisions or amendments: Executive Orders 12107, 12196, and 12564 and 5 U.S.C. chapters 11, 31, 33, 43, 61, 63, and 83. XRAY: Authority for Maintenance of X-Ray module: Includes the following with any revisions or amendments: Executive Orders 12107, 12196, and 12564 and 5 U.S.C. chapters 11, 31, 33, 43, 61, 63, and 83. **RTFM:** 5 USC 301, Departmental regulations
PIA - 8:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	**FCS:** N/A **FSTM:** OPM/Govt-10 - Empl Med File System Records **FedHealth:** Office of Personnel Management (OPM) Govt-10 Employee Medical File System Records **FMERITS:** 09-15-0004/ Office of Personnel Management (OPM) Gov **RTFM:** N/A
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains In-person Online Government Sources Within the OPDIV Other HHS OPDIV

		Other Federal Entities
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	**FSTM, FedHealth, FMERITS :** This program does not collect information from the public, and therefore, is not subject to the requirements of the Paperwork Reduction Act. **FCS and RTFM:** There is no OMB information collection approval number required to system administrators to have username and login to support an IT system.
PIA - 9B:	Identify the OMB information collection expiration date.	
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	**FSTM:** The notification process may differ slightly depending on the source where the records are obtained from, which may include: a. The

		individual to whom the records pertain b. Agency employee health unit staff c. Federal and private sector medical practitioners and treatment facilities d. Supervisors/managers and other agency officials. Other agency records. The ultimate point of data collection, however, is most often from the individuals in a clinic setting. In these situations, clients are provided with information and notifications in writing at the point of data collection. Individuals receive a Privacy Act Form at the point of data collection. Individuals ultimately provide their Personally Identifiable Information (PII) directly, and are aware of what PII they are delivering. Individuals are informed in writing via the Privacy Act notice of how the PII will be used or shared. **FedHealth:** 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. 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. **FMERITS:** All client agencies require employees or applicants to sign consent forms before collecting their data for FOH Medical Evaluation/Requirements Information Tracking System (FMERITS) . All employees are required to read FOH's privacy statement when they have their exams at the Occupational Health Centers (OHCs) and are asked to sign an authorization for disclosure which describes what information would be disclosed outside FOH (i.e., back to the client agency). Form FOH-6 is the disclosure form and form FOH-32 is the privacy statement. **FCS and RTFM:** When a system administrator takes a position administering IT systems, they are aware that they will need to login to an IT system to change the configuration and run security updates.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary

PIA - 13:	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	**FSTM:** Individuals can decide not to provide their PII however, they won't be able to have an examination. **FedHealth:** Individuals desiring employment will not be allowed to opt-out of the collection or use of their PII, as it is required to effectively store medical information, declining employment is an option. **FMERITS:** At the time of data collection, individuals are provided with a Statement of Understanding explaining how the information will be used, including an explanation that FOH staff will see the data entered into Occupational Health Information Management System (OHIMS) in order to make determinations about staff clearances. Once an individual's PII is in an FMERITS database, there is no way to opt-out. 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. **FCS and RTFM:** If desired, a system administrator could refuse the create a username and password. They would be unable to access or manage the IT system.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained	**FSTM:** There is not a mechanism in place to inform individuals when major changes occur to the system individually, although the Privacy Act System of Records Notice would be updated as needed. Individuals are informed at the point of data collection of all the possible uses and

		disclosures of their PII. At the time of record creation, individuals receive a Privacy Act form that informs them how their information will be used. Individuals may be required to supply information as a condition of their employment, but this is established by the client agency, not by a process that FOH controls. **FedHealth:** 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. **FMERITS:** All client agencies require employees or applicants to sign consent forms before collecting their data for FOH. All employees are required to read FOH's privacy statement when they have their exams at the Occupational Health Centers (OHCs) and are asked to sign an authorization for disclosure which describes what information would be disclosed outside FOH (i.e., back to the client agency). Form FOH-6 is the disclosure form and form FOH-32 is the privacy statement. **FCS and RTFM**: All system administrators would be aware of any major changes being made to a system. If a change was made without their knowledge the change would be documented in the change management log. Since no PII is stored on the system with the exception of system administrator's username and login created specifically for RTFM. The risk of a change creating an impact is minimal.
PIA - 15:	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. If no process exists, explain why not	**FSTM:** Individuals have the ability to object to the collecting clinic or agency. In addition, the FOH helpdesk can be contacted to receive complaints

		about privacy and security incidents. **FedHealth:** 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. **FMERITS:** There is a FOH process and policy to report a breach of PII. Any breach involving FMERITS should be reported to the FOH Helpdesk to start the process. As for inaccurate PII such as Date of Birth (DOB) or SSN, that information is brought to our attention by the employee or agency. The FMERITS team would then update the database with the correct information. If needed, review letters or other reports would be regenerated with the correct information. Any breach of Personally identifiable information (PII) and Protected health information (PHI) would be reported to Computer Security Incident Response Center (CSIRC), the FOH team would work directly with CSIRC. **FCS and RTFM:** If a system administrator was made aware that their username and password was used inappropriately they would be required to change their password. If the system administrator was not available, the account would be locked until their return.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not	**FSTM:** Annual system security assessments of this system are performed. The system has been through a security accreditation following National Institute of Standards and Technology (NIST)

		standards which Occupational Health follows in order to make ensure that system is compliant with the information system security standards that the government is required to follow. The NIST 800-53 document titled the Security and Privacy Controls for Federal Information Systems and Organizations is used to assess the confidentiality, integrity, availability, accuracy and relevancy 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 customer agencies are responsible for ensuring that the data is accurate and relevant. They can retrieve a report from FSTM that would list the individuals that have obtained services covered by the interagency agreement in a given month. **FedHealth:** 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 Point of Contact (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. **FMERITS:** Data is reviewed when new records are received to make sure the PII is accurate. Also, files are destroyed, returned to the client agency, and or sent back to the OHCs when no longer needed. **FCS and RTFM:** System administrator accounts are reviewed by the IT team monthly.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA-17	

	FSTM: 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. The majority of FSTM users are contractors, and use the data to track patients and bill the appropriate parties. System administrators and developers have access to verify the integrity of the data and ensure the availability of the system. **FedHealth:** Users Reasoning: Nurses and physicians in FOH health clinics are required to collect 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 Reasoning: 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. Developers Reasoning: Contractors Reasoning: 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 Reasoning: FOH Customer Call Center specialists will have minimal access to the PII data in order to support employees and end-users. **FMERITS:** Users Data Entry to enter medical records-review medical data and generate reviews Administrator: Account managers to track records - System Administrators have access to data for operations and support functions. Developers: Developers have access to data for support functions Contractors: Direct contractors have data access as administrators, developers and users. **FCS and RTFM:** System administrator need usernames and password to apply configuration changes and security patches to a system. They must authenticate to make these changes.	
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII	**FSTM:** 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. **FedHealth:** 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. **FMERITS:** Access to PII is granted based on roles. For example, if a system user will be responsible for only data entry and generate reports then the access will be granted under "User" category. **FCS and RTFM:** Only user that are tasked with administering RTFM will have username and passwords to login the system. RFTM will use roles to be sure each user has only the privileges needed to complete their job tasks.
PIA - 19:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job	**FSTM:** 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. **FedHealth:** 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. **FMERITS:** Role based access to the system and PII information is used to control read, write, or delete permissions. **RTFM:** RFTM will use roles to be sure each user has the minimal rights needed to complete their job.
PIA - 20:	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	**FSTM:** 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. **FedHealth:** All system users will complete required Annual HHS Security Awareness and Privacy Awareness Training. **FMERITS:** All system personnel depending on the roles receive the following HHS provided Cybersecurity and Privacy Awareness Training from the HHS Learning Portal (LMS). General training: HHS Cybersecurity Awareness Training Role-Based Training: Information Security for Executives Information Security for Managers Introductory Role-Based Training for IT Administrators **FCS and RTFM:** 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.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	**FSTM:** 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. **FedHealth:** 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. **FMERITS:** In addition to general security training, users receive training based on their roles. For example, system administrators will take IT Administrator's training. All of these trainings are provided by HHS. **FCS and RTFM:** There is no additional training.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s)	**FSTM:** The EMF (Employee Medical File) 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 30 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. **FedHealth:** PII data will not be deleted or purged from the system. All inactive information will be flagged with In-active Status. National Archives and Records Administration (NARA) General Records Schedules (GRS)-1 is the retention schedule for the FedHealth system. **FMERITS**: 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. 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. **FCS and RTFM:** System Administrator accounts are removed when a system administrator leaves, within 24 hours. There is no NARA guidelines for system administrators credentials retention.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response	**FCS:** FCS has both Unix and Windows based system. Unix based systems use a masked password shadowed files where the only visible

password will be a hash of the password. The hash is created from the password but the hash cannot be used to determine the password. When active directory Personal Identity Verification (PIV) login is available for Unix based systems, it will be used for FCS.
Windows systems require active directory PIV card login.
Administrative Controls: System Administrator accounts are reviewed monthly. The policy is always to give the least privileged to complete the tasks assigned. When a system administrator leaves their position FCS disables their account within 7 days.
Technical Controls: In a UNIX system roles are used to limit system access even among system administrators. For the Windows system active directory uses roles, assigned with the least privileged to complete the tasks assigned. Users can be added to a new group to complete a task and removed when that task is complete.
Physical Controls: This is an Amazon Web Service (AWS) system and has no specific physical location. The servers are replicated among AWS East server farms. During the Federal Risk and Authorization Management Program (Fed Ramp) qualification process, all server farms must meet Federal Government standards for building access, lighting and power requirements and locked spaces for networking, routing and server storage.

FSTM: 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.

FedHealth:

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.

FMERITS: Information in the system is protected by management, operational, and technical security controls commensurate with the level of sensitivity of the system, including: Physical Controls - All medical records are stored in a separate, locked file room. -All medical records are contained in Federal Government buildings that require Federal identification to enter. -All medical records are located within clinics that require pre-authorized access by Personal Identity Verification (PIV) card.
Technical Controls - Medical database files are protected by an internal firewall. - Internet Control Message Protocol (ICMP) is blocked on the internal pix firewall and the two SQL servers are configured not to reply to ping requests. - Audit trails are in place to monitor unsuccessful login attempts to the MEP module. - SQL servers are kept up to date with the latest security patches from Microsoft. - Only authorized internal domain users have access to the MEP database. - The firewall logs are routinely reviewed for unauthorized access. Administrative - Social Security numbers have been removed from all reports generated out of FMERITS. -All Health Insurance Portability and Accountability Act (HIPPA) rules are followed in all Clinics

RTFM: RMTF is a Unix based system. Unix based system uses a masked password shadowed files where the only visible password will be a hash of the password. The hash is created from the password but the hash cannot be used to determine the password.

PIA - 25:	Describe the purpose of the web site, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response	**FSTM:** FSTM provides a complete set of tools to define the interagency agreements between FOH and its customer agencies, collect evidence of the fulfillment of those agreements, and provide external financial systems the information they need to bill for services rendered. Federal Employees and Federal Contractors Public URL **FedHealth:** FedHealth is a web-based, occupational health and safety management system used to support the business needs of Federal Occupational Health (FOH). The system provides an electronic health record functionality to collect and document medical test results for federal employees enrolled in the medical clearance and surveillance program whose job requires them to meet specific medical requirements in order to perform their responsibilities safely. **FCS, FMERITS and RTFM:** N/A There are no website in FMERITS OR RTFM.
PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	No
PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	No