EPA United States
Environmental Protection
Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Medical Surveillance/Reasonable Accommodation

Preparer: John Jordan	**Office: Region 08, IMB, ISO**
Date: 01/25/2020	**Phone: 303 312 7072**

Reason for Submittal: New PIA____ Revised PIA____ Annual Review_X___ Rescindment ____

This system is in the following life cycle stage(s):

Definition □ Development/Acquisition □ Implementation □

Operation & Maintenance ☒ Rescindment/Decommissioned □

Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

Provide a general description/overview and purpose of the system:

This system is used to track applications by employees for services under the Occupational Medical Surveillance Program. Employees submit a copy of their request and the summary information, including a tracking number, of a medical evaluation carried out by a third party. This information is entered into a national system and the hardcopy forms are filed and kept under lock and key.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

Occupational medical surveillance, EPA ORDER 1460.1

National Oil and Hazardous Substances Pollution Contingency Plan 40 CFR Part 300, NCP

OSWER Directive 9285.3-12

Executive Order 12196

CERCLA section 105 (National contingency plan; preparation, contents, etc.); EPCRA section 305 (Emergency training and review of emergency systems); EPA Order 1440.2 (partial list: Occupational Safety and Health Act of 1970 and E.O. 12196, Occupational Health and Safety Programs for Federal Employees); EPA Order 1460.1 (partial list: 29 U.S.C. 655, section 6, and 29 U.S.C. 668, section 19, Occupational Safety and Health Act of 1970 and section 501 of the Rehabilitation Act of 1973, as amended). Purposes(s): Personal and Emergency Contact Information is used by line supervisors and managers of the RSC Program (1) to contact the RSC member in off-hours when he/she is needed to deploy to an incident and (2) in case of injury to the RSC member while deployed at an incident. Emergency planning, management and response-related training and certification information is used by individuals and managers of the various emergency management and response programs across the Agency to track required emergency response training.

Safety and health-related training and certification information is used by individuals and managers of the safety, health and environmental management program across the Agency to track required safety, health and environmental management training and medical monitoring data.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes. The system currently has an ATO. The ATO expired on September 15, 2019 and we are seeking a renewal.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR Required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service

(PaaS, IaaS, SaaS, etc.) will the CSP provide?

Information is entered into the national Emergency Management Portal (EMP) run by HQ. This PIA does not cover the EMP. It only covers the hardcopy forms retained by Region 08. The hardcopy data maintained by Region 08 is NOT STORED IN A CLOUD.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

Name, DOB, truncated SSN (last 4). This system does not collect medical information, it contains a reference to medical records compiled and maintained by another agency.

2.2 What are the sources of the information and how is the information collected for the system?

Information is provided by the FOH health unit and by the individuals on a manual (non-electronic) form.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

FOH data is verified by FOH, personal data is verified by the employee.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

Personnel gaining unauthorized access to the hardcopy files.

Mitigation:

Files are stored inside secured facilities and are further kept under lock and key. Only authorized employees have access.

Section 3.0 Access and Data Retention by the system

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

There are no controls granting separate access levels. Personnel with physical access to the files are designated by the Director of the Infrastructure Program in Region 08. Physical files are kept in locked receptacles inside secure facilities that require PIV access.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

Access is governed by Regional policy within the Infrastructure department.

3.3 Are there other components with assigned roles and responsibilities within the system?

No

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Local files are retained for recordkeeping purposes only. No personnel beyond the record keepers have access to the information. Data entered into the national system is controlled by the system owner at HQ. Access to the files is limited to EPA, non-contract, personnel.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Records are kept for the duration of employment plus 30 years. Per SORN EPA-70 this records schedule is still under development.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

Unauthorized access to records.

Mitigation:

Region 08 mitigates this risk by keeping the records inside the secure Region 8 headquarters building and further keeping the records in a locked container. Only authorized personnel have access to the

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Region 08 does not share this data. Region 08 does not control what the HQ application owner does with the data.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

This would be a high-level policy decision involving a Deputy Regional Administrator and HQ staff. Region 08 does not share this data and does not plan to do so.

4.4 Does the agreement place limitations on re-dissemination?

N/A

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

EPA does not share this data and does not incur a risk.

Mitigation:

None

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

5.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?

The system ensures that information is used in accordance with stated practices by limiting access to the information. Only employees and the designated data stewards are allowed access to the files. As the portion of the system maintained by Region 08 is manual process must be used rather than automation.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

Staff are briefed on PII policies and procedures when taking custody of the physical records. Annual PII training is incorporated into the mandatory IT training all employees must complete.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Unauthorized access to the records could result in unauthorized changes.

Mitigation:

Region 8 mitigates this risk by limiting access to designated personnel, allowing for rapid determination of the originator of any changes.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

Region 08 physical forms are submitted by employees to the designated data stewards. The data stewards use the forms to enter information into the national health and safety system. This information is used by HQ to track various health-related issues: safety of on-site response personnel, medical accommodations, and etc… The Regional responsibility is to enter the data into the national system. The data in the national system is covered by a separate PIA.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X__ No___. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other*

identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

Yes. Files are filed under the employee name.

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

These are the responsibility of the national system owner. EPA-70

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

The primary privacy risk to the physical records is unauthorized access by personnel inside the secure building.

Mitigation:

Region 08 has addressed this risk by physically securing the records in locked file cabinets, limiting the number of keys to these cabinets, and putting the keys in the hands of designated data stewards only. The Region 08 ISO has conducted a visual examination of the storage area and determined that the keys granting access to the files are themselves kept secured (in locked drawers and, in one case, also in a locked office).

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Unknown. FOH and EPA HQ administer this system and Region 8 is required to process forms when they are presented by personnel.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

Unknown. FOH and EPA HQ administer this system and Region 8 is required to process forms when they are presented by personnel.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

None.

Mitigation:

None.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Employees may request, by email or phone, and receive a copy of their file. Individuals must physically take delivery of their file after identifying themselves.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Employees may contact the record custodian to request changes.

8.3 How does the system notify individuals about the procedures for correcting their information?

It does not.

8.4 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

None.

Mitigation:

None.