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: Libby Asbestos Exposure Assessment Records	
Preparer: John Jordan	**Office: Region 08, IMB, ISO**
Date: 03/18/2020	**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 is an external hard drive containing medical information related to persons exposed to asbestos in Libby, Montana. This hard drive is locked in a file cabinet in an office in the Region 8 headquarters. It has not been accessed in over a decade. As the result of a court order due to pending litigation, Region 8 is not allowed to dispose of these records or send them to archive. Accessing this information would require locating special drivers and installing them on a computer.

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?

CERCLA, 42 U.S.C. § 9604(e)

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 has an existing ATO. The ATO was due to expire on September 15, 2019 and is in the process of being renewed.

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?

No.

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).

The system is not active and does not collect or disburse information. It is a copy of aggregated medical data supplied to the EPA by a third party in relation to the Libby Asbestos Exposure.

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

No information is collected. This data is on a removable hard drive kept in a locked cabinet. The information was provided to EPA by another agency as part of the Libby Exposure case. The information was originally provided by individuals who volunteered to participate in the Agency for Toxic Substances and Disease Registry (ATSDR) study on asbestos exposure in Libby, Montana.

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.

Data accuracy is not the responsibility of the EPA, Region 08. Data was provided by a third party. This data was not collected on the behalf of EPA, it was collected by another agency for their use and a copy was provided to EPA who determined that it was not needed but was prevented from disposing of it by a litigation hold.

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:

None. Data kept on hard drive in locked secured cabinet. Data is not access and is on hold due to ongoing litigation.

Mitigation:

None.

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?

Yes. The data is kept locked in a cabinet in a secure building and is never connected to any electronic devices.

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 entirely physical and is limited to the Information Security Officer, Chief of the Technical Services Unit, and one staffer from the Records center. No one is allowed to access the data and they would be unable to do so without significant effort. A chain of custody form is used to record custody of the data set.

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?

The three people identified in 3.2 have physical access to the hardware on which the data is retained. The data itself is not accessed by anyone and could not be accessed without significant technical effort.

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.

The information will be retained until released by court order. Records are retained under schedule 0014.

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:

Someone might steal the hard drive.

Mitigation:

Keep the hard drive locked in a file cabinet inside an office inside the key-card secured facilities of the Region 8 HQ building in Denver.

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.

No.

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

Data is not shared externally.

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?

The region reviews automated information sharing via our weekly change control process. Sharing of the data contained on this drive would require a request for physical access to the drive which would be reviewed by the Information Security Officer, Liaison Privacy Official, and the director of the Records Center.

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:

None. The data is not for sharing.

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 information is retained due to a court order. The Region ensures the data is not used improperly by limiting access to the hard drive containing the information and keeping the hard drive locked in a storage container and unconnected to any electronic devices and power sources.

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

All Region 08 personnel are required to take annual Information Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Information might be used in discordance with authorized purpose.

Mitigation:

Any request to access this data would require a thorough review by senior staff.

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.

The information is not used.

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.)

A SORN has been published indicating that information in this system can be retrieved by individual identifier. No one who has seen the actual data is still employed by EPA and we cannot confirm this. Efforts at anonymization were made by the agency (not EPA) that gathered the data but no details are available.

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

SORN EPA-48

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:

Someone might use the information for an unauthorized purpose.

Mitigation:

We keep the drive locked in a filing cabinet to prevent this.

*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.

Notice is not provided because the system does not actively collect information.

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?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are set out in 40 CFR Part 16**.**

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:

Because there are no policies related to data collection it's possible data might be collected without providing proper notifications.

Mitigation:

We are mitigating this by not collecting data to add to this data set.

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?

Requesters will be required to provide adequate identification, such as a driver's license, employee identification card, or other identifying document. Additional identification procedures may be required in some instances.

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

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are set out in 40 CFR Part

16.

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

Individuals who want to know whether this system of records contains a record about them, who want access to their record, or who wants to contest the contents of the record, should make a written request to the System Manager.

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:

Because EPA did not collect this data it is possible subjects were not provided with the appropriate information regarding their ability to opt-out of collection.

Mitigation:

None. EPA did not collect this data and is not collecting more data for this data-set.