United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO Roster.docx

System Name: Occupational Health Software Safety System (OHSSS)		**System Owner:** Eileen Arnold	
Preparer: Eileen Arnold & Sylvette Garnes		**Office:** EPA/OFA/SIMD/MOB	
Date: 6/11/26		**Phone:** 202-564-1313	
Reason for Submittal:			
New: X	Revised: ☐	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: X	
Operation & Maintenance: ☐	Rescindment/Decommission: ☐		

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:

The Office of Real Property, Safety and Security (ORPSS) has contracted with a FedRamp approved Cloud Service Provider (CSP) to implement a Software as a Service (SaaS) solution for an EPA digital data Medical and Occupational Health tracking and workflow management system. This system will result in improved efficiency for EPA to meet its regulatory requirements while providing robust oversight of the occupational health of agency employees. Additionally, this solution will provide for the ongoing systematic collection, storage, analysis, and interpretation of employee medical and exposure data, fulfilling the purpose and intent of EPA Order 1460.1 (OMSP), OSHA-medical surveillance requirements. The Office of Finance

and Administration (OFA) - Office of Chief Facilities and Security Officer (OCSFO)- Safety and Occupational Health Division (SOHD) - Medical Occupational Health Branch (MOHB) has a contractual agreement with Cority Software Inc. Cority is the FedRamp Authorized CSP that provides the SaaS solution for the EPA. Cape Fox Endeavors is a participant in the MOHB overall solution and (formerly known as Eagle Health) provides expert medical services to EPA, including medical examinations and clearances, in support of (SOHD's) safety, health, and environmental programs, including EPA's Occupational Medical Surveillance Program (OMSP). MOHB collects and stores data from EPA employees on paper forms that are stored in locked offices (e.g., EPA employee paper medical records received by former medical services vendor, Federal Occupational Health. EPA discontinued services with FOH effective September 2025, these paper medical records are being processed to send to EPA's Digitization Centers for scanning) and on electronic (scanned) forms stored in MOHB's SharePoint site previously approved to handle sensitive (medical) PII. This PIA documents the change in storage of EPA personnel health data to include EPA's MOHB Medical SharePoint site. OFA-OCFSO-SOHD-MOHB will use the data collected by Cape Fox Endeavors in support of EPA's OMSP medical evaluation program. In addition, MOHB uses the Medical SharePoint site to manage several other activities: Pre- and Post- Deployment medical evaluations, incident related post exposure assessments, Travel Health consultations and additional activities which include reviewing agency Reasonable Accommodation cases, Voluntary Leave Bank cases, Worker's Compensation cases and injury/illness tracking, and Medical Employability. OFA-OCFSO-SOHD-MOHB is required to collect this medical information to ensure EPA employees are healthy and safe while performing mission-essential duties. The information collected by Cape Fox Endeavors on behalf of OFA-OCFSO-SOHD-MOHB supports EPA employees' health and safety while they accomplish EPA's mission to protect human health and the environment.

The following forms are used by Cape Fox Endeavours to collect medical related information from EPA employees on behalf of MOHB: OMSP Part A, Part B and Part C which includes an Authorization for Disclosure Statement as part of these forms.

Section 1. 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 Safety and Health Act of 1970, 5 U.S.C. 7901, 29 CFR 1910.1020, 20 U.S.C 657, EPA Order 1460.1

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?

No. This is a new FISMA system.

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, N/A

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?

Yes. The CSP is FedRamp authorized. This is a SaaS solution.

Section 2. Characterization of 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).

Information collected on the following forms is voluntary but may impact employment or job assignment should they decline the medical examination. Thus, most employees will undergo the medical examination.

Full name, DOB, Email, Agency Employee Number, and other related medical exam information (such as blood type). No SSN information is collected.

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

EPA employees, and contract employees (emergencies only).

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, the system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

- OMSP Part A - Employee completes and certifies. Supervisors review and certify. Safety and Health Environmental Manager Program (SHEMP) Managers review and certify.

- OMSP Part B - Employee completes and certifies. Medical Examiners review and certify.

- OMSP Part C (Medical Clearance Statement) - Reviewing physician certification. The Medical Clearance Statement Form is completed by MOHB Reviewing Medical Officers (RMO). Cape Fox medical administrators perform quality checks on full exam packets to ensure all required medical information is complete before sending the information to MOHB for final review. EPA's medical team has performed this function since receiving clearance in 2023 for storing medical PII on SharePoint.

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 who provide information to complete the various forms do not provide accurate information. Unauthorized personnel gain access to PII data captured on paper or electronic forms and alter this data.

Mitigation:

Data entered on the various forms are certified as correct by Cape Fox and EPA officials. Medical records are kept in secure, access-controlled buildings. Paper copies are in locked offices. In the future, there will be electronic forms to capture the same information

Section 3. 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. Users must authenticate to access EPA network and authorize to use specific SharePoint folders to store PDF files. When medical information is initially captured on paper forms, OFA-OCFSO-SOHD-MOH personnel store this information in locked cabinets in locked offices. Paper copies are scanned to PDF. The resulting PDF copy containing OMSP Part A, B and C will be stored in EPA's SharePoint folders. Part B contains S-PII therefore the SharePoint Access Control List is different than SharePoint folders used to store Part A and C data. Safety, Health, Environmental Management Program (SHEMP) Guideline 57 document has a detailed overview of the OMSP program. SORN EPA-64 is the system of record for privacy data stored on SharePoint.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Information in paper form is kept in locked offices. Only Cape Fox personnel with the correct key are allowed access. Once this information is copied to SharePoint, Role Based Access Controls (RBAC) are used to ensure only authorized EPA and Cape Fox personnel are allowed access to designated folders on the SharePoint site based on MOHB management area of responsibility and an Access Control List (ACL). Access can be revoked or edited by the site owner. The ACL groups determine the roles and what information can be accessed by users.

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

No, not currently.

3.3 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?

Cape Fox Medical Personnel are external to EPA. OFA-OCFSO-SOHD-MOHB. MOHB personnel (*Medical and Occupational Health Branch*) engaged Cape Fox via contract agreement. The following FAR clauses are included in the contract agreement. FAR 42.302, FAR 42.1502, and FAR Subpart 34.2.

NOTE: Division Supervisors and agency Region Program Safety and Health Environmental Manager Managers (SHEMP) have access to non-sensitive PII only.

3.4 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.

Per EPA Order 1460.1, medical records are kept at least 30 years post EPA employment. The program office follows EPA Record Schedule 0566.

3.5 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:

There is a risk that an individual's records are stored over 30 years post EPA employment.

Mitigation:

OFA-OCFSO-SOHD-MOHB personnel will monitor, and track employee medical record stored in an agency database to ensure records that exceed 30 years post-employment are removed. Records are sent to NARA per the record schedule.

Section 4. 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 governments, 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.

EPA has a contract agreement with Cape Fox Endeavors which is managed by OFA-OCFSO-SOHD-MOHB. MOHB collects information on various paper forms on behalf of EPA via Cape Fox medical services clinic network. This information is saved as a PDF file and uploaded to EPA's SharePoint site.

Paper copies of employee medical records previously collected by FOH, EPA's former medical services provider, are retained by OFA-OCFSO-SOHD-MOHB in locked cabinets. The paper copies are being prepared by MOHB to be sent to EPA Digitization Centers to be scanned with the electronic files attached to employee records in OHSSS once it is fully implemented. Cape

Fox ensures all current EPA medical exams information is kept in an employee's electronic medical folder in MOHB's Medical SharePoint site until OHSSS is fully implemented. Per EPA policy these electronic medical folders will be archived to the National Archives and Records Administration as an employee retires/separates from EPA or leaves the OMSP program.

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

There is no external sharing. Just data transfer from Cape Fox to OFA-OCFSO-SOHD-MOHB. MOHB has medical staff collecting employee health information and OMSP parts A, B, and C medical information on behalf of EPA. This information is then used by EPA to meet OMSP program requirements. OFA-OCFSO-SOHD-MOHB provides essential medical examination/clearance for EPA employees, technical assistance from physicians to ensure EPA employees are healthy and safe while performing mission-essential duties. MOHB AUD form is hand carried by the employee to the clinic and then placed into the appropriate paper medical record file. Currently the program uses paper collection, but it is moving to an electronic interface. MOHB shares non-sensitive information with EPA Safety and Occupational Health Division personnel. MOHB will send full medical records information eventually to NARA when the documents are archived.

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?

Contact agreement between Cape Fox and EPA (OFA-OCFSO-SOHD-MOHB).

4.4 Does the agreement place limitations on re-dissemination?

Section III.6.a of the Contract Agreement between Cape Fox and MOHB does not allow for re-dissemination of medical information. EPA will send full employee medical information to National Archives and Records Administration (NARA) for archiving purposes.

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:

Unauthorized access to medical information collected by CapeFox on behalf of EPA (OFA-OCFSO-SOHD-MOHB).

Mitigation:

Via the Contract Agreement, information collected by Cape Fox is not shared outside EPA (OFA-OCFSO-SOHD-MOHB). In addition, information that Cape Fox collects on behalf of EPA is locked in a cabinet and the room also is locked. Only Cape Fox personnel with a key to the room and the cabinet have access.

Section 5. 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 as stated in Section 6.1?

Medical information that Cape Fox captures from EPA personnel on paper copies are in locked rooms. Only Cape Fox personnel with a key can access this information. Once Cape Fox personnel complete the exam procedures for an EPA employee, the required forms are completed, and a workflow process begins that results in an adjudicated medical clearance. This clearance and the appropriate forms are scanned as PDF files and then Cape Fox personnel save this information to EPA via MOHB's secure SharePoint site. OFA-OCFSO-SOHD-MOHB authorized personnel then move this information to a SharePoint folder. Role based access is used for the SharePoint components. There are strict Standard Operating Procedures (SOPs) set in place to handle this type of employee data.

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

EPA users are required to take the annual mandatory Information Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

Medical data collected by Cape Fox become available to unauthorized personnel or to EPA personnel without a need to know.

Mitigation:

This is a paper-based system thus no electronic audit logs are available. However, Cape Fox POC Account Management Assistant (AMA) performs a quality review of the medical exam package before scanning the information for uploading to EPA (MOHB) secure SharePoint site where EPA MOHB personnel review and audit.

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

In occupations identified as having risk potential, track the employees' health status over time to detect and respond to any relevant deviations that may occur. Determine if the deviation relates to exposure to occupational stresses. Ensure that employees who are assigned physically demanding work have the

physical capacity to perform their regularly assigned duties without endangering their own safety and health, or that of their co-workers or the public. Accumulate, analyse, interpret, and disseminate information, when appropriate, on trends in disease and injury incidence and/or prevalence as they relate to specific hazardous exposures or to defined work activities.

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.

Information identified on OMSP Part A, B, and C will be retrieved by Agency Employee ID, Full Name, Phone Number, and Email. MOHB collects and store information under the government-wide OPM-GOVT-10 SORN. When information is saved to SharePoint, EPA-64 SORN is used to provide coverage. OPM Govt 10 (Employee Medical Records) SORN has been previously cleared by IT Security review using the OPM Gov't 10 (Employee Medical Records) SORN to support the new computerized process.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

Controlled access to facilities protects individual privacy. The program uses locked rooms for file storage. Once the medical records are digitalized, role-based access will be activated to only allow people who have a need to know to access the data in their official duties.

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:

Personnel use the medical records for other reasons than intended purposes. In addition, there is always a risk of misuse of information by both authorized and unauthorized users of O365 / My Workplace.

Mitigation:

Role based, and multifactor authentication access will ensure that only authorized EPA personnel with a need to know will have access to medical records. SharePoint Access to customer data is also strictly logged, and both system and database administrators perform regular security audits (as well as sample audits) to attest that access is appropriate.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

Individuals are notified that they're not compelled to complete OMSP forms Part A, B or C. However, not providing the information may affect the availability and quality of health services rendered to a person and may also affect the completeness of information used by MOHB or EPA in making determinations of medically related employment decisions.

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:

Individuals are not provided with any notice that Cape Fox and EPA will collect their health data.

Mitigation:

Before collecting medical information, employees selected to participate in OFA-OCFSO-SOHD-MOHB safety and medical program are informed that their health information will be collected as related to agency mission.

Section 8. 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?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted.

Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40

CFR part 16.

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 described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 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 Freedom of Information Act (FOIA).

Privacy Risk:

The program does not provide additional redress beyond the Privacy Act and FOIA requests afforded to individuals.

Mitigation:

N/A

I attest as the Agency Privacy Officer that **Occupational Health Software Safety System (OHSSS)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.06.22 12:07:35 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt. Branch
EPA/OFA