

# PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)

(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%20Roster.docx](https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx)

<b>System Name:</b> Public Health Emergency Workplace Response System (PHEWRS)	
<b>Preparer:</b> Gloria Meriweather	<b>Office:</b> Office of Mission Support
<b>Date:</b> January 13, 2021	<b>Phone:</b> 202-566-0652
<b>Reason for Submittal:</b> New PIA <input checked="" type="checkbox"/> Revised PIA <input type="checkbox"/> Annual Review <input type="checkbox"/> Rescindment <input type="checkbox"/>	
<b>This system is in the following life cycle stage(s):</b>	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input checked="" type="checkbox"/>	
Operation & Maintenance <input type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
<b>Note:</b> 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 <u><a href="#">OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</a></u>	
<b>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u><a href="#">OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</a></u></b>	

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

EPA proposes to establish a new system of records to manage the Agency’s planning and response to a public health emergency in EPA locations. EPA intends to collect information in the system to assist EPA with maintaining safe and healthy workplaces, to protect individuals in EPA locations from risks associated with a public health emergency, to plan and respond to workplace and personnel flexibilities needed during a public health emergency, and to facilitate EPA’s cooperation with public health authorities.

## **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?**

Executive Order 12196, Occupational safety and health programs for Federal employees (Feb. 26, 1980) 5 U.S.C. 301 “Departmental Regulations”, 8 U.S.C 1101, 1103, 1104, 1201, 1255, 1305, 1360; 44 U.S.C. 3101 “Records Management by Federal Agency Heads.”

**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, ServiceNow system security plan has been completed for the information system supporting this system. Yes, the system has been issued an Authorization-to-Operate. The ATO expires March 11, 2024.

**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 Information Collection Request (ICR) is 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?**

Yes, the data will be maintained stored in a cloud. The CSP, ServiceNow - ServiceNow Service Automation Government Cloud Suite, is FedRAMP approved. The CSP provides SaaS.

**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 following is a list of Data Elements in Contact Tracing application used when the Contact Tracer is filling out needed fields. *All location based and phone related data elements listed in the table below are explicitly associated with business location details unless otherwise noted.*

<b><u>Data Elements</u></b>				
<b>Field Label</b>	<b>Column Name</b>	<b>PII</b>	<b>Sensitive PII</b>	<b>PHI</b>
Program/Region		X	No	
Work location		X	No	
Employee status			No	
EPA email		x	No	
Business Phone		x	No	
Best contact number		x	No	
Supervisor		x	No	
supervisor email		x	No	
supervisor phone number		x	No	
Person		x	No	
Create New		x	No	
My Cases		x	No	
All Cases for my CT team		x	No	
Open Cases for my CT team		x	No	
unassigned Cases for CT team			No	
ALL		x	No	

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

Contact tracing team collects information from federal employees as they voluntarily provide health information. All participants will be able to provide data through their reporting supervisor as well as provide data to designated contact tracer. The information in this system is collected both from the individual and from the individual's emergency contact.

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

All data provided by employees to the Contact Tracing team are personal artifacts and not publicly sourced data.

## **2.4 Discuss how accuracy of the data is ensured.**

The EPA Contact Tracer asks a series of questions to confirm the caller's identity, according to the Contact Tracing Team Standard Operating Procedures (SOP).

Information is checked for accuracy through self-verification by either the user or the EPA Contact Tracer entering the information to process an omission of contact. EPA Contact Tracing Team personnel ensures data accuracy in EPA Public Health Emergency Workplace Response System through program, the data fields in the input screen are configured to limit the possibility of entering malformed data (e.g., the system rejects 000/000/0000 phone numbers). Only authorized personnel or EPA Contact Tracer can review and edit information prior to and after their submission with permission of the employee this is not mandatory.

## **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:**

Data element information entered by contact tracers could contain erroneous data because of input error.

### **Mitigation:**

Verifying data input in fields is valid by responsible contact tracer.

## **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 preventative access controls within EPA ServiceNow enforced with application role-based controls. These role-based controls provide separation of duties and limits access to data within the application to only EPA personnel. The assigning of roles enhances adherence to the principle of least privilege for access to data.

**Access control levels are dictated by roles that have been assigned/ designated by EPA. The roles are as follows:**

- Sr manager
- Region manager
- Contract tracer

Sr manager roles are assigned by the cloud service provider whose responsibility to grant/remove access for region managers. Region manager roles are to grant and remove access to assigned/designated contact tracers.

Contract tracer roles have limited access to view/enter data and have not permissions to grant or remove users.

Technical controls exist to separate responsibilities and permissions based on the roles assigned. Cloud instance databases are separated by firewall preventing any access to separate instances of service now. The contact tracing instance is technically disjoint from all other instances of the overarching application.

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

These access controls are documented in ServiceNow knowledgebase also in the EPA COVID-19 site under guidance documents. Access control to the contract tracing system is initially provisioned and designated by the SNOW cloud administrators.

**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?**

EPA ServiceNow, and the data contained within, will not be accessible to any external parties (i.e. the public, outside agency, or external companies/contractors).

All Contact Tracers will have access to internal data, having valid credentials and assigned roles.

Necessary FAR clauses have been included in the EPA EUS contract that was awarded to SAIC in March of 2017

**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.**

Public Health Emergency Workplace Response System retained information will be deleted or destroyed when the Agency determines they are no longer needed for administrative, legal, audit, or other purposes This is done in accordance with EPA Policy to help support after-the-fact investigations. EPA ServiceNow is under EPA Records Control Schedule 1012 and 1049.

### **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:**

There is a risk that information may be retained longer than needed.

#### **Mitigation:**

Public Health Emergency Workplace Response System adheres to Records Control Schedule 1012(b) and 1049 associated with its data.

## **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.**

Public Health Emergency Workplace Response System does not share information externally.

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

Public Health Emergency Workplace Response System, EPA-89 does not share information.

### **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?**

Public Health Emergency Workplace Response System, EPA-89 does not share information.

### **4.4 Does the agreement place limitations on re-dissemination?**

Public Health Emergency Workplace Response System, EPA-89 does not share information.

### **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. There is no external sharing either than the routine uses.

**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 as stated in Section 6.1?**

Public Health Emergency Workplace Response System ensures that practices stated in the PIA are followed by leveraging training, policies, EPA Rules of Behavior, and auditing and accountability. EPA security specifications require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All EPA systems employ auditing measures and technical safeguards to prevent the misuse of data.

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

The US EPA implements a Rules of Behavior (ROB) for which all users must consent prior to being granted systems credentials for access. The system inherits the EPA implementation of User Information Security and Privacy Awareness training which is provided annually. In addition, all EPA personnel receive annual refresher cybersecurity training to educate them regarding the use and management of sensitive data.

### **5.3 Privacy Impact Analysis: Related to Auditing and Accountability**

**Privacy Risk:**

There is a risk that some Public Health Emergency Workplace Response System users may not complete required training.

**Mitigation:**

This is mitigated through policies that disables a user's account access to the EPA for not completing all required training, disabling a user's account also removes access to EPA ServiceNow. EPA ServiceNow IT personnel is required to complete training before access is granted to any additional roles.

## **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 EPA uses the data collected by EPA Public Health Emergency Workplace Response System to provide pandemic support and other data tracking and reporting activities to

support EPA health and wellness as well as support a safe working environment for employees onsite. EPA Contact Tracing Team use a user's information to provide support for EPA employee safety, assets, and properties. Service orientated activities include the following:

- Managing records submitted by employees
- Retrieving incident and contact information
- Managing IT Assets
- Conveying pandemic information from across the enterprise.

**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.)*

The system retrieves information using EPA employee name, email address and phone number.

**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?**

EPA Privacy Act System of Records Notice(s) EPA-89 applies to EPA Public Health Emergency Workplace Response System.

The following information is to be provided and agreed to by the end user:

The EPA has implemented several types of evaluation cases for determining how to protect the privacy of individuals within Public Health Emergency Workplace Response System, EPA-89. The information's primary purpose is used for collecting de-identified statistical pandemic information to promote awareness and workplace safety. By analyzing and providing various security tools that exist within the ServiceNow cloud application. This includes access control lists, role-based access controls. The EPA adheres to the privacy act of 1974 and all applicable governing bodies. Vulnerabilities can be mitigated in order to correct any deficiencies in terms of privacy controls. The ServiceNow infrastructure is scanned every 72 hours for vulnerabilities, and the Contact Tracing application is part of that ServiceNow SaaS infrastructure being scanned which is on the ServiceNow platform.

**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:**

There is a risk that unauthorized users may access records in EPA ServiceNow.

There is a risk that EPA ServiceNow could be used for purposes outside the scope of the Contact



Tracing Team.

**Mitigation:**

This risk is mitigated. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards such as restricting access to authorized personnel who have a need-to-know. Users must authenticate their credentials to gain access to the system.

Prior to gaining access to the system, EPA ServiceNow displays a warning banner contact tracers will disclose the following statement (The purpose for the collection will be to provide the necessary data for proper medical evaluation and diagnosis , to ensure that proper treatment is administered, and to maintain continuity of medical care. Collected information will only be disclosed to those that have a need to know, where there is a compelling circumstance affecting the health or safety of an individual.) Contact tracers will be presented with the login screen to advise all users about proper and improper use of the data, that the system may be monitored to detect improper use, and the consequences of such use of the data. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. This acts as a deterrent to unauthorized activity.

The risk is mitigated through role-based access rules governing technical support personnel usage. Only EPA contact tracing team has access to forms or data fields required to access portal to create a data record from employee.

**\*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.**

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](mailto: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?**

Contact Tracers will inform employees that information being collected is intended for the sole purpose of ensuring the safety of the EPA workplace. The information will not be shared with anyone else. Employees will be informed that their participation in contact

tracing is voluntary. Employees have the option of refusing to participate. They also have the option of having their identity masked in the contact tracing application. The system will allow us to enter “John Doe” as a case name and will populate “dummy” information rather than the employee’s actual organization, supervisor, and workstation location.

### **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:**

A low risk exists for contact tracers skipping over mandatory scripts in order to inform the users of the divulgence of information such as PII/PHI. There also may not be enough detailed information to educate the user in those banners/warnings through a lack of policy guidance.

#### **Mitigation:**

Contact tracers are required to read a script warning participant of the risk of divulging PII/PHI. Contact tracers are trained to give assurance of the safety and security of the collection of data.

## **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?**

Any individual who wishes to know whether this system of records contains a record about themselves, and to obtain a copy of any such record(s), should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, [privacy@epa.gov](mailto:privacy@epa.gov).

### **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 FOIA.*

**Privacy Risk:**

Little to no risk. Public Health Emergency Workplace Response System will leverage established EPA procedures for redress and follow SORN procedures.

**Mitigation:**

EPA will always provide access and amendment of Public Health Emergency Workplace Response System for individuals. 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