United States Environmental Protection Agency

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

System Name: BenCloud	**System Owner: Neal Fann**
Preparer: Liz Etchells	**Office: OAR-OAQPS-HEID-RBG**
Date: 10/15/2021	**Phone: 919-541-0732**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ 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:

BenCloud will be a tool for EPA and non-EPA users to calculate and monetize the health impacts of air pollution changes. Users will provide maps of baseline air quality and air quality under an alternative scenario such as a proposed policy change. BenCloud will calculate the change in health impacts due to the change in air quality. The information to calculate the change in health impacts comes from published epidemiology literature which studies the distribution and determinants of health-related conditions or events in specified populations. The health information is aggregated and does not include any individual health or personal information. The change in health impacts is then used to calculate the economic benefits or costs of the change in air quality.

BenCloud will be a cloud-based version of the current software tool BenMAP which has similar functionality. BenMAP is used to support Regulatory Impact Analyses (RIAs). In the future, EPA staff

will use BenCloud for RIAs.

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?

The Clean Air Act of 1990 and Executive Order 12866.

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-Use? When does the ATU expire?

We are pursuing an Authorization-to-Use.

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.

The information is not covered by the Paperwork Reduction Act. User information will be limited to those disclosures that require users to provide or display only facts necessary to identify themselves, in this case their name and email address in order to distinguish the individual account. All user provided data is voluntarily provided and will not be collected or aggregated.

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. We are using IaaS native AWS solutions for hosting containers, API, etc. We are using EPA's version of AWS. This AWS is FedRamp certified.

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).

BenCloud's collected information will be directly provided by users through the web interface. BenCloud will use user-provided maps of air quality and user-input analytic choices such as what health outcomes to value. It will store these in user accounts. The data elements collected are

- User account identifier – First name and last name
- User email address – User's choice to provide either a personal or business email.

- Air quality map(s). These are two dimensional surfaces, either gridded or based on political boundaries such as counties, with measures of pollution in each location.
- Analytic choices. These include which health outcomes to value (e.g. mortality, lung cancer), what scientific models to use, how to combine scientific outcomes, and how to aggregate and display results.

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

There are three sources of information in BenCloud. First is user provided data. All user provided data is voluntarily provided. Users provide maps (surfaces) of air quality. They may also specify particular analytic choices such as which health outcomes to model. User information can be provided by EPA and external users. Second is third party data such as population maps. This is provided by EPA after being procured from third parties such as other federal agencies. Third is scientific information such as the functions mapping air quality to health outcomes and the valuations of specific health outcomes. This is provided by EPA based on Agency staff's review of the scientific literature.

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

Yes. The system uses commercial and publicly available data on political jurisdictions (county, state, and country borders), population (by racial group), and baseline health outcomes. For example, the tool uses population data from the U.S. Census Bureau; baseline rates of death and disease from the Centers for Disease Control and Prevention and the Healthcare Cost and Utilization Program; and projected rates of economic growth from the Bureau of Economic Analysis. Each dataset is publicly available and does not contain personally identifiable information.

2.4 Discuss how accuracy of the data is ensured.

Accuracy of the data is not directly assessed. It is left up to each user to ensure the accuracy of the information they enter into BenCloud.

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:

The primary risk to the characterization of the data is human error, which could result in the entry of inaccurate data by the user. The character of the information is low risk. The user's name and e-mail address is the only information that can be used to distinguish an individual.

Mitigation:

There will be a built-in check to verify usernames and email addresses to mitigate any risk of inaccurate data.

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. Each user has a username and password to prevent access by unauthorized users. Users can share data with other authorized users, including by placing data into a shared repository.

Users with a "manager" account type will be able to see resource use statistics (total resource use, resource use by account). The manager account is to monitor our financial liability to the cloud provider and, if necessary, limit external users in order to avoid incurring excessive AWS bills.

Users with "administrator" accounts will be able to see individual users' data including uploaded air quality surfaces, analytic options selected, outputs, and error logs. This is primarily for ongoing debugging and development.

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

Each user will receive an email when they first set up their account. These access controls will be documented in the initial email as well as in an instruction manual and privacy statement which will be available online.

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

The assigned roles and responsibilities are:

- **Manager**: Managers are responsible for ensuring that BenCloud is not incurring excessive costs.
- **User**: These users are responsible for performing air quality benefits analyses. They may choose to share data with other users.
- **Administrator**: Administrators who are responsible for system maintenance and ongoing development.

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?

Users who have set up accounts will have access to their own data including uploaded air quality surfaces, analytic options selected, outputs, and error logs. EPA BenMAP staff (e.g. Neal Fann) and the contractors (currently Industrial Economics (IEc)) will have system administrator accounts and will have access to the above information only for the purpose of system administration and diagnosing user support issues. These contractors are covered by the Rights in Data clause (FAR 52.227-14).

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.

No EPA records are created by this application. There is no applicable schedule. (RLO confirmed in writing)

3.6 Privacy Impact Analysis: Related to Retention

Privacy Risk:

Retaining data indefinitely presents a risk of data being exposed in a scenario like an unauthorized data breach. This risk was weighed against the irreversible damage that would be caused by data loss in a scenario where an organization's collected information was automatically purged before they had a chance to make a backup copy.

Mitigation:

As detailed throughout this PIA, significant efforts have been taken to secure the system from a technical perspective against unauthorized access and/or data breach. Furthermore, training and documentation will encourage users to create backups and delete data which is not used for RIAs within 3 years of creation, as a general guideline. Even though this won't be strictly enforced by the system, it is expected that training and education will make this a standard practice so that in reality most records are deleted by users within 3 years of creation.

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, the application does not share any PII data externally. For non-PII data, EPA users of BenCloud will be using the tool to run analyses of EPA regulations and programs. The

results of these analyses would be entered into EPA documents including Regulatory Impact Analyses (RIAs), Technical Support Documents (TSDs), or other similar regulatory documents. Non-EPA users may choose to share their analytic results as part of reports or studies for their own purposes. Typical non-EPA users include state air agencies, other governmental users, and non-governmental organizations (NGOs) such as charity or advocacy organizations.

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

Not applicable.

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?

Not applicable.

4.4 Does the agreement place limitations on re-dissemination?

Not applicable.

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.

Mitigation:

Not applicable.

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?

The system's security model, as described above, ensures that each user only has access to the information they are authorized to view. This enforces the roles and access described throughout this PIA.

EPA staff and EPA's developer contractor regularly review the practices stated in this PIA to ensure ongoing compliance.

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

Privileged users will receive annual Information Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a risk that a glitch or defect in the systems security code theoretically may allow access to unauthorized users, which would undermine the technical safeguards enforcing the procedures outlined in this PIA.

Additionally, there is a risk that EPA or its contractor's staff may inadvertently act out of accordance with the procedures outlines in this PIA.

Mitigation:

BenCloud will undergo quality assurance testing to ensure that the security model is behaving correctly and limiting access to information to only authorized users. Furthermore, automated and manual test suites are regularly performed on each new version of the system to ensure continued operation as expected.

EPA staff and EPA's developer contractor regularly review the practices stated in this PIA to ensure understanding of and ongoing compliance with this PIA's practices.

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 will not be directly accessed by EPA. The only exception is that EPA's administrator and developer contractor may need to access information in response to a user support request, but in that case they would only be accessing the information for diagnostic purposes.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No_X_. 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 organizes information by user account. Once logged in, a user will be able to retrieve their previous analyses by file name. Previous analyses include user uploaded air quality modeling surfaces and analytical choices in BenCloud. Saving these previous analyses allows the user to make changes to an analysis, if needed, without starting the process from scratch. The system is not designed to retrieve information by personal identifier and users cannot load other user's data without permission.

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 controls are technical and administrative. Only EPA's system developer contractors (IEc) have security access to the servers, code and databases.

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:

Risk EPA employees would access data and misuse the information.

Mitigation:

The risk is mitigated by limiting the stored data to user id's, email addresses, air quality information, health analysis modeling choices, valuation results and simulated population health results.

***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.

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?

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:

Mitigation:

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?

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

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:

Mitigation: