# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

04/07/2025

### OPDIV:

ACF

### Name:

PREP PLUS

**PIA Unique Identifier:**

P-4725518-344866

**The subject of this PIA is which of the following?**

Minor Application (stand-alone)

**Identify the Enterprise Performance Lifecycle Phase of the system.**

Operations and Maintenance

**Is this a FISMA-Reportable system?**

Yes

**Does the system include a Website or online application available to and for the use of the general public?**

No

**Identify the operator.**

Contractor

**Is this a new or existing system?**

New

**Does the system have Security Authorization (SA)?**

Yes

**Indicate the following reason(s) for updating this PIA.**

**Describe the purpose of the system.**

he purpose of this task order is to support high quality performance measurement for the Personal Responsibility Education Program (PREP), which is administered by the Family and Youth Services Bureau within the Administration for Children and Families (ACF) of the U.S.

Department of Health and Human Services (HHS). As part of the task order, the Contractor will develop a Performance Measures Data Portal and Performance Measures Dashboard that will incorporate de-identified individual-level data. The Performance Measures Dashboard will function as an interactive reporting and analysis tool designed to improve data-driven decision-making for PREP program administrators and grantees. The Contractor will also revise existing measures (program participation rates, demographic data of participants and youth behavioral outcomes) used to monitor and report grantee performance; analyze and report performance data; and support PREP grantees in continuous quality improvement related to biannual performance measures reporting. The revision process evaluates, updates, and integrates performance measures with stakeholder input and testing before implementation.

**Describe the type of information the system will collect, maintain (store), or share.**

The system will directly collect and store the following types of information: User account information (including name, email, and phone number), grantee-level data, and provider-level data.

The following types of information will be collected outside of the system then uploaded and stored in the system: performance measures, including data about grantees, providers, and programs and de-identified participant-level entry and exit survey data. Results as masked to prevent possible re-identification.

**Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.**

The system consists of a web portal with an integrated dashboard and a public informational website. Access to the web portal and dashboard is restricted to registered system users, while the informational website remains publicly accessible.

User information, including name, email address, and phone number, is collected to establish secure accounts for program officers, grantees, and providers. The web portal allows registered users to input grantee-level and provider-level data. Additionally, grantee users upload de-identified participant-level survey data collected externally from youth, which includes demographic data and information about the participant's sexual intentions and behaviors.

After each data submission period, grantee-reported performance measures are removed from the Data Portal and permanently added to the Dashboard. All Personally Identifiable Information (PII) is managed according to the system's retention and destruction procedures.

**Does the system collect, maintain, use or share PII?**

Yes

**Indicate the type of PII that the system will collect or maintain.**

Name
E-Mail Address
Phone Numbers
Youth responses to survey questions, including demographic characteristics and questions about sexual intentions and behaviors.
Performance measures, including data about grantees, providers, and programs and de-identified participant-level entry and exit survey data.

**Indicate the categories of individuals about whom PII is collected, maintained or shared.**

Public Citizens
Business Partner/Contacts (Federal/state/local agencies)

**How many individuals' PII is in the system?**

100,000-999,999

**For what primary purpose is the PII used?**

User account information: User information including name, email address, and phone number is collected for the purpose of establishing accounts for users to securely access the web portal and

dashboard.

Survey data: Responses to survey questions are used to provide the program office and grantees with the data on the youth they serve through PREP programs.

**Describe the secondary uses for which the PII will be used.**

The secondary use is to provide performance indicators for annual Office of Management and Budget (OMB) reporting.

**Identify legal authorities governing information use and disclosure specific to the system and program.**

PREP is authorized and funded by Section 513 of the Social Security Act (42 U.S.C. § 713), as amended by Section 50503 of the Bipartisan Budget Act of 2018 (Pub. L. No. 115-123) extended by Division CC, Title III, Section 302 of the Consolidated Appropriations Act, 2021 (Pub. L. No.116-260).

**Are records on the system retrieved by one or more PII data elements?**

Yes

**Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.**

System number is 09-80-0361, titled “OPRE Research and Evaluation Project Records,” that is

**Identify the sources of PII in the system.**

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Non-Government Sources

Other

**Identify the OMB information collection approval number and expiration date**

OMB Control No. 0970-0497. Current Expiration Date: 07/31/2026.

**Is the PII shared with other organizations?**

No

**Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.**

User account information: Individuals request an account which requires them to provide their name, email address, and phone number for creating and maintaining an account.

Survey data: All survey data is collected by grantees outside the system. ACF instructs grantees to contact an Institutional Review Board (IRB) to obtain a determination letter for their proposed data collection procedures. Grantees choose their own IRBs. Therefore, the details of the data collection procedures can vary by grantee in accordance with the determination of the grantee’s overseeing IRB. After grantees administer the surveys, they upload de-identified survey responses to the system using a file upload feature.

**Is the submission of PII by individuals voluntary or mandatory?**

Voluntary

**Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.**

User account information: Individuals who need an account for the portal and dashboard to perform their work must provide the personal information required to create and maintain an account. An

individual can opt-opt of requesting an account.

Survey data: Details of the survey data collection procedures are determined by grantees and their overseeing IRBs outside of the system. The cover page of the survey indicates that participation in the survey is voluntary, and that youth may skip any questions they do not feel comfortable answering.

**Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.**

User account information: Personal information is only used for the purpose of user account creation and maintenance. System changes would not impact how this PII is used within the system.

Survey data: Grantees are notified of any changes to the system and instructed to contact their IRBs to determine any implications for their participants.

**Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.**

User account information: An account invitation email will be sent to all new users. If an individual has concerns that the account was established inappropriately, they can contact the help desk to resolve the issue.  A link to the help desk will be provided in the email.

Survey data: The de-identified survey data is collected from youth outside of the system by grantees who are the direct contacts for individuals participating in the program. Grantees are instructed to follow the data collection procedures they establish with an overseeing IRB.

**Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.**

Integrity: Each user has their own unique login with specific permissions based on their task. They can only access areas of the system that are required for their work.

Availability: The system is configured with redundancy, high availability, and monitoring of system resources leveraging services of the Federal Risk and Authorization Management Program (FedRAMP) certified cloud service provider.

Accuracy: Key fields must be completed to proceed with a task. Where applicable, fields have edit checks to ensure that data are provided in the correct format. Radio buttons, drop down menus, calendar functions and other common system features are used to ensure that responses are limited to the range of acceptable data for a given item.

Relevancy: Mathematica project staff confirm that the user account email addresses are complete and, if not, they contact the program and ask them to reinforce to the individual the importance of getting complete contact information.

**Identify who will have access to the PII in the system and the reason why they require access.**

**Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.**

User account information: Administrators and developers may access PII to resolve account access

issues that may arise.

Survey data: Only system developers and research programmers have access to the individual survey responses maintained in the system. Other systems users can view only tabulated data displayed in the integrated dashboard and programmed reports.

**Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.**

Role based permissions are applied within the system to restrict those with access to PII based on the principle of least privilege which provides them with the minimum amount of information needed to perform their job.

Grantee users only have access to the data associated with their grantee, and provider users only have access to the data associated with their provider.

**Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.**

All personnel with access to PREP PLUS receive general Cyber Security Awareness Training (CSAT) annually, ensuring they are informed about cybersecurity best practices. Those with significant information security roles undergo role-based security training before gaining system access, whenever there are major changes to their role or the system, and at least once per year to maintain proficiency. All trainings include certification to verify completion and compliance with security requirements.

**Describe training system users receive (above and beyond general security and privacy awareness training).**

The indirect contractor, Mathematica, provides training webinars, a written manual of operations, and written guidance documents, along with help desk support. The manual of operations and guidance documents are reviewed and updated as needed twice per year to ensure accuracy and relevance. For technical assistance, PII is used solely for sending email announcements and reminders and for responding to Help Desk requests submitted by grantees. For the portal and dashboard, PII is used solely for establishing and maintaining user accounts. Access to these systems is restricted to ACF staff, grant recipients, and their partners. To enforce these restrictions, we create individual user accounts, which require PII due to the multifactor authentication process. For all of these uses, PII is limited to name and contact information (email address and in some cases phone number).

**Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?**

Yes

**Describe the process and guidelines in place with regard to the retention and destruction of PII.**

All PII will be destroyed 3 years after cutoff. Cutoff occurs when the data containing PII becomes obsolete, is superseded, or is no longer needed to support program actives. (DAA-0292-2016-0014 2.2.)

**Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.**

Administrative Control: Access to Personally Identifiable Information (PII) is restricted using Role-Based Access Control (RBAC), ensuring users only have the minimum permissions necessary, following the principle of least privilege.

Technical Control: Data is encrypted both in transit and at rest. In transit, data is secured using HyperText Transfer Protocol Secure (HTTPS) with Transport Layer Security (TLS) 1.2+, ensuring safe communication between users and the system. At rest, data is protected using the Advanced Encryption Standard (AES-256) encryption algorithm. Additionally, Multi-Factor Authentication (MFA) is enforced for web portal login to enhance security.

Physical Control: The system inherits the physical security measures implemented by its Federal Risk and Authorization Management Program (FedRAMP)-certified Cloud Service Provider (CSP), ensuring compliance with federal security standards.