# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

02/06/2024

### OPDIV:

ACF

### Name:

Regional Partnership Grant Evaluation Data System

**PIA Unique Identifier:**

P-6526053-146327

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

Major Application

**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?**

Existing

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

Yes

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

PIA Validation

**Describe in further detail any changes to the system that have occurred since the last PIA.**

The following functional changes were made to the system:
Updated data validation rules
Added new video tutorials
Increased file size upload limit

**Describe the purpose of the system.**

The Regional Partnership Grant (RPG) Evaluation Data System (EDS) will collect data on the enrollment, implementation, and baseline and follow-up outcomes of the RPG program. The RPG program requires the Department of Health and Human Services (HHS)/Administration for Children and Families (ACF) to evaluate and report on the effectiveness of the grants. Under ACF, the Children's Bureau (CB) funds and oversees the RPG program and will use the information in RPG-EDS to track how 1) grantees are using the funds, 2) leveraging their resources through partnerships, and 3) serving their clients. The results of the evaluations contribute to the

understanding of how best to serve families addressing substance use issues and improving the well-being of and permanency outcomes for children affected by substance abuse. CB is required to report the findings to Congress on a biennial schedule beginning in 2018.

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

The RPG-EDS will collect and store the following types of information about the RPG program: Grantee organizations will create case records to report on the clients enrolled in their programs and services provided. After the case is created, the grantee can add case members (clients) at any time and assign a unique client Identification (ID) for continued reference. Each adult and child record are required to contain the client's name, date of birth (DoB), enrollment date, gender, and person type (adult or child). The adult and child records may contain race, ethnicity, primary language, level of education completed, employment status, source of income, primary residence type, relationship status, household member(s) type, child's expected birth date (if unborn), focal child statistics, and case closure details (once services have ended). Additionally, service logs are created that link to a client record by ID that contain the name of the service provider dates, service location, approach, type of service, focus area(s), referral type, length of service, and engagement level.

On a semi-annual basis, grantees submit administrative data on child safety and permanency, and adult recovery. Child safety and permanency information includes type of abuse and/or neglect, dates of report, incident, and/or placement, type and frequency of substance abuse, removal date and reason, and placement dates and setting. Adult recovery information includes Dates of treatment and discharge, reason, substance type(s), and frequency of use(s).

Also semi-annually, grantees submit standardized instrument data from the following instruments: (1) Infant-Toddler Sensory Profile, for children aged 0 to 36 months, which provides a standard method for measuring a child's sensory processing abilities (such as an over- or under-response to stimuli, including loud noise, light, or touch) and measuring the effect of sensory processing on functional performance in a child's daily life; (2) Child Behavior Checklist-Preschool and School-Age Forms for children aged 1.5 to 18 years old, which collects information from caregivers to assess children's behavior and emotional and social functioning; (3) Adult-Adolescent Parenting Inventory-2 which assesses attitudes about parenting and child-rearing; (4) Center for Epidemiologic Studies-Depression Scale, 12-Item Short Form, which is a screening tool that assesses the presence and severity of depressive symptoms of caregivers; (5) Addiction Severity Index, Self-Report Form which assesses the severity of parental drug and alcohol abuse; and (6) Trauma Symptoms Checklist-40, which is optional for grantees to administer, and measures aspects of post-traumatic stress and other symptom clusters in adults. All standardized instruments are self-administered and scored and interpreted the same way per the instrument developer's guidelines.

For individuals with a system account, including grantees, service providers, and technical team users (Indirect contractors), the following information is collected and stored: name, email address, phone number, password, and role. For grantee users, specifically, their grantee organization ID is also collected.

All data in RPG-EDS will be stored on the records retention schedule approved by the National Archives and Records Administration (NARA) (Disposition number DAA-0292-2019-0007).

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

The RPG-EDS will collect data on the enrollment, implementation, and baseline and follow-up outcomes of the RPG program. ACF/CB is required to evaluate and report to Congress on the effectiveness of the grants on a biennial schedule which includes how the grantees are using the funds, how their resources are being leveraged through partnerships, and how grantees are serving their clients. Information collected includes case and client-specific information entered by the grantee after each enrollment. The adult and child information may include race, ethnicity, primary language, level of education completed, employment status, source of income, primary residence type, relationship status, household member(s) type, child's expected birth date (if unborn), focal child statistics, and case closure details (once services have ended). Additionally, service logs are

created that link to a client record by ID that contain the name of the service provider dates, service location, approach, type of service, focus area(s), referral type, length of service, and engagement level.
Grantee organizations also submit standardized instrument data and administrative data used by CB to evaluate the wellbeing outcomes of families participating in services. Outcomes data submissions are made by grantee organizations semi-annually on child safety concerns, adult recovery statistics, and standardized survey results on adult-adolescent parenting, infant-toddler sensory profiles, child behavior, epidemiological studies on depression, trauma symptoms, and addiction severity.
All data in RPG-EDS will be stored on the records retention schedule approved by the National Archives and Records Administration (NARA) (Disposition number DAA-0292-2019-0007).

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

Yes

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

Date of Birth
Name
E-Mail Address
Phone Numbers
Medical Notes
Employment Status
User Credentials
Demographics (race, gender, ethnicity)
Grantee Organization ID
Grantee Users

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

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

10,000-49,999

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

The primary purpose of the PII collected on the clients served is to calculate age in years and months. This information is critical to score the instrument according to age-based norming tables and interpret the standardized instruments per the instrument developer’s guidelines. The primary purpose of the PII collected on the RPG-EDS users is to establish and maintain a user account.

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

There are no secondary uses for the PII collected.  PII is not displayed in any documentation or reports. All report findings are presented at the aggregate level.

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

The Child and Family Services Improvement and Innovation Act (Public Law 112-34).

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

No

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

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Other

Government Sources

State/Local/Tribal

Non-Governmental Sources

Public

Private Sector

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

OMB control number: 0970-0527

Expiration date: 04/30/2025

**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.**

The grantee organizations are the source of information collection and are responsible for the notification to individual's that their personal information is being collected. As part of conducting an outcome evaluation, each RPG grantee is required to develop a consent form to be formally reviewed and approved by its local Institutional Review Board. The grantees are expected to obtain active consent from each individual prior to that individual's participation in the local and cross-site evaluation project.

For individuals from grantee organizations that require a user account with RPG-EDS (additional grantee administrators or service providers), they are asked by the grantee administrator in each grantee organization to provide their business email and phone number in addition to their full name for account set-up. Individuals providing this information for an account understand it is collected by the system to create and maintain the account. For technical user accounts, those are limited to the vendor's technical team. Those individuals undergo the same process as other users and understand the system collects their information for the purpose of creating and maintain an account.

**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.**

Individuals who are volunteering to participate in the RPG local and cross-site evaluation project are given the option to opt-out at any stage of the program or evaluation. All consent forms contain statements that explain to the program participants that there are no penalties for choosing to not participate or to not answer specific questions and that the individual can withdraw from the study at any time. If an individual previously provided consent and then chooses to withdraw that consent, RPG will no longer use that data upon the participant's notification.

Individual's that require a user account in RPG-EDS may or may not be able to opt-out of the collection of their personal information depending on their job responsibilities. For this reason, the information is limited to only what is required for account creation and maintenance.

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

Major changes to any data collection or use by RPG-EDS are distributed via notification from the CB Deputy Associate Commissioner to each grantee primary point of contact. The grantee is then responsible for continued notification to the program participants. Any data changes are then reviewed by CB to determine updates that may be required to their documentation, including the Office of Management and Budget (OMB) information collection approval package, privacy impact assessment (PIA), and/or consent forms.

Major changes involving system functionality or an interruption in service for the system are communicated directly to system users via email and a notice is posted on the system login page. System users can reply to the email notification, if they have concerns, but are not required to respond to acknowledge or consent to the changes as these types of changes do not affect data disclosure, collection, or use.

**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.**

Any program participants that believe their personal information has been inappropriately obtained, used, or disclosed, or that the information is inaccurate will contact the grantee organization where the information was initially collected. If the grantee cannot resolve the issue or believe this to be a suspected or confirmed privacy incidents, they will contact the CB technical team. For system users, RPG-EDS allows for self-maintenance of account information to maintain accuracy and provides a help desk email address on the system landing page and footer as well as a telephone number provided in training material to report any concerns in data collection, use, or disclosure. Any suspected or confirmed privacy incidents will be reported to the ACF incident response team to ensure proper review and investigation

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

The following processes and methods are in place for RPG-EDS data:
Data accuracy is the responsibility of the grantee organization that is entering the program participant information into the system. There isn’t a periodic review process in place to confirm the accuracy of this information.

For user account information, the users can review and edit their own information to ensure accuracy.

To ensure data availability the database is backed up for point in time recovery for 35 days and monthly snapshots are taken and retained for 1 year.
To ensure data integrity the system has validation rules implemented for all data entered and stored in the database. In addition, role-based access controls what data users have the ability to modify.

To ensure data relevancy the grantees who collect the data are responsible for entering the data into RPG-EDS and a number of CB users are granted the ability to edit participant data as needed. User account login history is reviewed, and inactive accounts are then disabled after 180 days of inactivity. All user accounts are reviewed and confirmed or updated on an annual basis.

**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.**

CB has established business rules to address who may access and have write ability for the data in RPG-EDS. Grantees and service providers are responsible for the input of PII and are restricted to only the cases they are reporting on under their grant. The technical team, which includes CB staff and Indirect contractors, have access to all records for oversight and system operations and maintenance.

**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.**

Access is limited to the functions and information which is essential to complete the user's job requirements. Role-based access control (RBAC) is used to limit read and write access through the system interface and back-end.

**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.**

Both Federal staff and Indirect contractors are required to take annual security awareness training, which includes privacy awareness topics. Training for federal staff is administered and tracked by HHS/ACF and contractors have the training administered and tracked by the company. All grantee organizations participating in the program are required to train their teams on security awareness and human subject's protection by local institutional review boards (IRBs).

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

To orient users and prepare them to use the RPG-EDS, the CB RPG-EDS team provides initial system specific training to all users. The training includes security awareness topics and best practices around data security and privacy. CB will administer and manually track the completion of this training.

**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.**

The following retention timeline has been approved by NARA: All records will be cut off upon completion of the final report or termination of research. The records will then be transferred to the National Archives 5 years after cutoff. The assigned disposition numbers are: DAA-0292-2019-0007-0001, DAA-0292-2019-0007-0002, and DAA-0292-2019-0007-0003.

Additionally, the following general records schedule (GRS) dispositions are followed for RPG-EDS system access and backup records: DAA-GRS-0006-0003, DAA-GRS-0006-0005, and DAA-GRS-0006-0006.

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

RPG-EDS is hosted on the Azure Government cloud platform certified by the Federal Risk and Authorization Management Program (FedRAMP). The PII in RPG-EDS will be secured in the following ways:

Administrative controls, including:

Security authorization, file backup/archive, user manuals, contractor agreements, training, and risk analysis.

Technical controls, including:
User Identification and Authorization via username and strong password requirements, multi-factor authentication (MFA) provided by Twilio and Google Authenticator, which combined provide options via text, voice, and smartphone application (app) with or without Internet access, Transport Layer Security (TLS) 1.2 enabled for all communication to and from the system, databases encrypted using Transparent Data Encryption (TDE), storage service encryption enabled for all storage, Virtual Machines (VMs) encrypted using Bitlocker, Azure Log analytics enabled to collect and analyze data generated by cloud resources (database/storage/Virtual Machines), and vulnerability scans using Tenable.io Web Application Scans (WAS).

Physical controls are inherited from Azure and include:
Access approval required at the facility's and building's perimeter and within the building and each data center floor, access request and approval process, perimeter fences, video monitoring, physical security staff, two-factor authentication with biometrics, and full body metal detectors.