US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/10/2025

OPDIV:

ACF

Name:

Recruitment, Enrollment and Study Delivery tool (RESD)

PIA Unique Identifier:

P-5718623-019843

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?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

Administration for Children and Families (ACF) desires to carry out a large, national-scale evaluation effort aimed at better understanding the effectiveness of recovery coaching interventions for parents with substance use disorder (SUD) who are involved with the child welfare system. The evaluation includes two recovery coaching program models: the Parent Mentor Program (PMP) and Sobriety Treatment and Recovery Teams (START).

The evaluation will consist of two independent impact studies. One will test the impact of PMP (in four states) on parent well-being (e.g., substance use, parenting stress) and child welfare outcomes (e.g., foster care placement, family reunification, subsequent maltreatment). The other will test the impact of START (in up to six states) on child welfare outcomes (e.g., foster care placement, family reunification, subsequent maltreatment). The evaluation will also include implementation studies to document local contexts, fidelity, and frontline practices and shed light on the ways they may intersect with program impacts.

The R3 (Replication of Recovery and Reunification Interventions for Families-Impact Study) project will support the impact and implementation evaluations; it will cover participant outreach; participant consent and enrollment in the study; collecting survey data, administrative data, and implementation data.

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

The R3 project data will consist of the R3 Analysis Data and the R3 implementation data that are processed and stored in two interconnected systems: the Career Pathways Extended (CPE) that was already accredited by ACF, and the Recruitment Enrollment and Study Delivery tool (RESD).

The R3 Analysis Data will be processed and stored in the Career Pathways Extended (CPE) system that was already accredited by ACF. The R3 Analysis Data consists of participant identification information (name, date of birth, Child Welfare identifiers, last four digits of Social Security Number), confirmation of informed consent, participant contact information, name and contact information for alternate contacts. The R3 Analysis Data will also include participant responses to the baseline and follow-up surveys that are conducted in CPE. The surveys will collect information about a participant' s experiences, thoughts, and feelings around substance use, child welfare, and well-being (e.g., mental health, quality of life, social support, housing and economic circumstances). The surveys will also collect demographic information (e.g., sex, race, ethnicity, education, and employment). Data analysis will be conducted within CPE by the evaluators.

The R3 implementation data will be processed and stored in the Recruitment Enrollment and Study Delivery tool (RESD). The implementation data will include group assignment, administrative child welfare records (e.g. child welfare services received and child welfare case status/outcomes), Medicaid records (e.g. health services received), and information about intervention service receipt (e.g., type, mode, duration of peer recovery coaching contacts). Participant outreach, participant consent, and enrollment in the study will be done in RESD.

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

The R3 Impact project will use two interconnected systems which are both hosted and managed only by the direct contractor, Abt Global.

The first system called the Recruitment Enrollment and Study Delivery tool (RESD) is used for study recruitment, study enrollment, ongoing contacts, and tracking intervention service receipt. This system is built to the Federal Information Security Modernization Act (FISMA) Moderate standard in accordance with FIPS 199 and complies with Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA). Abt Global has custom built this system and is responsible for its security.

RESD is a combination of three components:

Case Management Tool (CMT) built on Appian which has been accredited as a Platform as a Service provider by FedRAMP and addresses the Federal Risk and Authorization Management Program (FedRAMP) security control requirements that are aligned to the NIST 800-53, Rev. 5 security control baseline for Moderate impact level as the Credential Service Provider (CSP). CMT is a business process management tool utilized for managing study enrollment, assessing study eligibility, collecting participant consent, designating treatment and control groups, and services tracking. The CMT designates user roles, including admin privileges for managing user accounts, and existing users. Appian user accounts will be centrally managed in the CMT and access to study participant details limited by user role and group. CMT will collect basic participant details (name,

date of birth, sex, race, language, ethnicity), identifying information from the child welfare system, alternative contact information, and types of services provided to participants. The CMT will allow users to report on services provided, re-assign participant records, and document service delivery outcomes. Participant information is assigned to a single program, with access restricted to users associated with the program. Each program is categorized by state, and user permissions are assigned at either the state or program level.

Random Assignment Generator (RAG) built on AWS which addresses the FedRAMP security control requirements that are aligned to the NIST 800-53, Rev. 5 Security control baseline for Moderate impact level. The Random Assignment Generator is utilized for ensuring a 1 to 1 treatment/control ratio is assigned for each participant. A unique project id is created in the Random Assignment Generator and associated with the client system. Each project sets up the input fields and overall ratio of assignments for treatment and control groups to process participant information. The participant identifier, project identifier and randomization criteria are passed through the Application Programming Interface (API). The client system stores the category options for associating strata criteria with individual participant information to randomize assignments and display results.

Microsoft Entra ID is the authentication system used for user authentication and access management within RESD. Microsoft Entra ID is the new name for Azure Microsoft Active Directory inside the Azure cloud environment.

The second system called Career Pathways Extended (CPE) is already accredited by ACF, it is used for survey data collection, storage, and analysis of study data. CPE is a single multi-tenant environment built to the FISMA Moderate standard by Abt Global for use on its projects. The entire environment is built on Amazon Web Services (AWS) using various infrastructure as a service (IaaS) and platform as a service (PaaS) offering from Amazon. CPE has been categorized as a Moderate impact level system, in accordance with FIPS 199 and complies with HIPAA, FERPA, and FISMA Moderate standards. AWS addresses the FedRAMP security control requirements that are aligned to the NIST 800-53, Rev. 5 Security control baseline for Moderate impact levels.

These two systems (RESD

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

Yes

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

Social Security Number
Date of Birth
Name
Driver's License Number
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Education Records

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?

500-4,999

For what primary purpose is the PII used?

PII will be used (1) to conduct outreach to potential participants, (2) to conduct tracking outreach and update contact information in support of the follow-up survey, (3) locate study participants for the follow-up survey, and (4) to match study participants to administrative data records.

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

There are no secondary uses for the PII.

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

42 U.S.C. § 1310

Public Law 115-271; (SUPPORT for Patients and Communities Act)

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.

09-80-0361. OPRE Research and Evaluation Project Records -9/19/2022

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

Identify the OMB information collection approval number and expiration date

OMB 0970-0616 - Replication of Recovery and Reunification Interventions forFamilies-Impact Study (R3-Impact)

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

The study team will establish memoranda of understanding (MOUs) with sites participating in the evaluation to outline roles and responsibilities for study activities. The study team will also establish data use agreements (DUAs) with each study site to document the data elements that will be shared and processes and protections for data sharing.

Describe the procedures for accounting for disclosures.

The PII in the system will be accessed only by personnel with authorization to view the data. All intended disclosures of this information will be documented via a contract, Memorandum of Understanding (MOU), or similar.

In the event of an unintended disclosure, the R3 Incident Response Plan will be activated. This existing Plan includes the procedures to follow including notifying ACF, OPRE, and Department of Health and Human Services (HHS) of any security incidents.

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

Individuals will be provided the opportunity to opt into the study (it is voluntary). Should they choose to participate in the study, they will sign an informed consent form that describes the collection and use of personal information.

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

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.

Study participation is voluntary. Submission of PII (name and contact information) is required for all study participants. Individuals who opt into the study will consent to sharing PII with the evaluators. Because study participation is voluntary, participants will be required to provide PII (name, contact information, date of birth) to evaluators for data collection purposes. This information is needed to link study participants to administrative data records and to contact them for the follow-up survey.

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

Since the PII is only used for providing a means to contact participants, confirm identity, and link participants to administrative records, any system changes would not impact them directly. As a result, there would not be a need to notify them or obtain consent. If there was a major change that would require notification and new consent, the individuals would be contacted via the email or phone number associated with their account.

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.

At the time of consent, participants will be given contact information for the study director and the Abt Global IRB. If a participant believes that their PII has been inappropriately obtained, used, disclosed, or is incorrect, they will notify the project director or Abt IRB. Study participants can also use the Abt IRB toll-free number to call if they have concerns about improper usage of data or their rights as a study participant. If a subject contacts Abt Global with a concern, Abt Global and OPRE together will conduct an investigation and reach a resolution including whether to remove or correct the information in this database and/or any other databases (where the data originally resides).

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 PII of the Participants will be reviewed for accuracy as part of the initial contact process. The other PII in the system is related to the individuals who are using the system directly (users).

Data Integrity is ensured through role-based access control which limits the number of privileged users that can view or change PII. Log files are maintained for any changes that occur within the system and are monitored for changes.

Data availability is handled by the infrastructure. The system is hosted inside the Amazon Web

Services (AWS) East/West Cloud environment which provides high availability using multiple availability zones, creating redundancy. The data is backed up daily.

Data Accuracy is ensured through built in quality control standards requiring all data to be entered in a correct and usable format. The individual user will ensure that their name and contact information is correct when the account is first created.

Data Relevancy is maintained by following the specific retention schedules as required by NARA.

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.

Access to PII is restricted only to those users who need it. For example:

Survey interviewers, managers, and individuals who work in the call center (Call Center Personnel) need access to PII for validation purposes.

Analysts need access to PII for matching administrative data sources.

Analysis staff have access only to deidentified data.

The Project Director must approve everyone who receives access to a project folder containing PII and the folder(s) that they can access.

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.

The entire system restricts access to PII using privileges assigned to their system account. For example:

Only individuals identified as Administrators have access to manage accounts belonging to other individuals.

Call Center Personnel, child welfare staff, and program staff only have access to the systems that they need to perform their work.

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 RDS receive general security awareness training, and personnel with significant information security roles receive role-based security training, at least (a) before they receive access to the system, (b) when there are major changes to their role or system, and (c) on at least an annual basis.

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

Staff that work with study participants complete Institutional Review Board (IRB) training through the Collaborative Institutional Training Initiative (CITI). The CITI training is valid for three years. All survey data collection team members are trained in the specific study procedures; how to login and access the data for the project, how to safeguard their equipment, how to report any suspected incidents. Staff conducting administrative data collection do so in accordance with the guidance

established in the data use agreements that govern that collection of information.

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 Contractor (and/or any subcontractor) shall maintain all information in accordance with DAA-0292-2012-0001 (Sequence Number 3.1), Child and Family Services Reviews.
Records generated from assessments, on-site reviews, Program improvement plans and final reports. Disposition Instruction: Temporary - Cutoff at the end of fiscal year and destroy no sooner than 10 year(s) after cutoff, but longer retention is authorized. Disposition Authority Number: DAA-0292-2012-0001-0005

In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with HHS/NIH policies.

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

The ability to change or create PII (name and email and contact information for users) is limited based upon least privilege and only granted to privileged users of the system.

Administrative Controls include requiring general security awareness training to be completed by all users plus additional role-based security for privileged users of the system.

Technical Controls include role-based access, positive user identification, passwords, multi-factor authentication, least privilege access, and all the intrusion detection services provided by Amazon Web Services.

Physical Controls are inherited from the hosting cloud and include all the security controls for a commercial data center (security staff personnel checks, visitor access procedures, intrusion detection system, fire suppression, uninterruptible power supply (UPS), climate controls, etc.)