US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/17/2024

OPDIV:

ACF

Name:

Next Generation of Enhanced Employment Strategies (NextGen) Project

PIA Unique Identifier:

P-4270862-324503

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.

The Next Generation of Enhanced Employment Strategies (NextGen) Project will identify and rigorously evaluate innovative interventions designed to promote employment and economic security among people with complex challenges to employment. The project is using an experimental design in which eligible individuals who consent to participate in the study are randomly assigned to either an intervention group, which can receive services from the intervention being studied; or a control group, which cannot receive those services but can receive other services in the community. The project will follow study participants over time and collect information about their earnings, employment, and other outcomes to determine the effectiveness of the interventions.

The NextGen Project team and programs participating in the project rely on the NextGen project system, which consists of the Random Assignment, Participant Tracking, Enrollment and Reporting® (RAPTER) and Survey Management System (SMS). RAPTER will be used for collecting information, performing random assignments, administering surveys, and tracking service receipts. SMS will be used for storing and managing information related to study participants.

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

The system will collect, maintain (store), and/or share the following types of information about study participants:
Identifying information (such as name, date of birth, Social Security number (SSN);
Contact information for the respondent (such as telephone number(s), Mailing address(es), email(s), social media handles) and other individuals who may The system will collect, maintain (store), and/or share the following types of information about study participants:
Identifying information (such as name, date of birth, Social Security number (SSN);
Contact information for the respondent (such as telephone number(s), address(es), email(s), social media handles) and other individuals who may know how the respondent can be contacted (name (s), Mailing address(es), and telephone number(s));
Demographic, socio-economic, and health characteristics of the study participants at the time of random assignment (including employment status, public benefit receipts, criminal justice system involvement, substance use information, and information regarding any disabilities);
and services received by treatment group members of the program.

This information will be used to describe the study sample; as baseline data in the impact analysis; to construct subgroups for the impact analysis; reach sample members for follow-up surveys; obtain updated contact information for sample members; match sample members with their corresponding administrative data; monitor for study participants reapplying to the program; prevent the program from providing services to members of the control group; and describe the services received by the treatment group.

In addition, RAPTER stores the name, email address and telephone number for each RAPTER user, including those staff conducting random assignment and entering service receipt information at the sites being evaluated. This is needed to maintain security and access controls to RAPTER.

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

RAPTER is a cloud-based, Internet-facing, web application into which programs participating in the NextGen Project enter information about sample members. RAPTER performs random assignment of sample members into treatment or control groups and allows programs to record treatment group members' participation in program activities and services.

The SMS is a Mathematica custom-built, web-based application, which enables status tracking of sample member interviews. The SMS is a contractor internal application and is not Internet facing.

The records retention schedule for these records is DAA-0292-2016-0014 2.2. These records are temporary and will be destroyed 3 years after cutoff. Cutoff occurs when the records become obsolete, are superseded, or are no longer needed to support program activities.

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
E-Mail Address
Mailing Address

Phone Numbers
Employment Status
Social Media Handle(s), Demographic, Socio-economic,
Health characteristics of the study participants,
Public benefit receipts, Criminal justice system involvement,
Substance use information, Information regarding any
disabilities.

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

Public Citizens
Programs -non government entities

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The primary purpose for the PII collected from respondents is to prevent participants from being enrolled into the study multiple times; to reach sample members for follow-up surveys; to obtain updated contact information from friends and relatives; to uselocating databases for sample members who cannot be located with the contact information they provided at study enrollment; and to match sample members with their corresponding administrative data. The employment status and other variables collected at enrollment are important to define the subgroup and to use in estimating the impact of the program. The PII from RAPTER users is used to maintain security and access controls to RAPTER.

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.

Section 1110 of the Social Security Act (42 U.S.C. § 1310

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.

9/19/2022

09-80-0361. OPRE Research and Evaluation Project Records.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Other Federal Entities
Non-Government Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date

OMB approval number: 0970-0545
Expiration date: 4/30/2026

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.

We will have data use agreements in place with the selected programs -HHS (NDNH data), SSA, state and local agencies (for other administrative data) and locating service/data broker - for confirming and updating participant contact information.

Describe the procedures for accounting for disclosures.

While a procedure for accounting for disclosures is currently not in place, the project team will work with the vendor to develop a procedure for accounting for disclosures.

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 are read a study consent form before they enroll in the study. This form lists the information being collected about the study participant and describes how the information will be used.

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.

The study consent form explains that participation is voluntary and provides information on how to opt out of the study at any time. To withdraw from the study, study participants must first call Mathematica, then write a letter or email indicating their intention to withdraw from the study, and send the letter to the address on the consent form.

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

Once the applicants are officially enrolled in the study, Mathematica will have the ability to contact the applicants directly. In the event that planned disclosure and/or data uses have changed, Mathematica will contact and re-consent the applicants under the updated conditions.

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.

If an individual is concerned that their PII has been inappropriately obtained, used, or disclosed, they may contact Mathematica directly. A toll-free telephone number for the study is provided to the study participants on the consent form. The study participant may also contact a representative of the program being evaluated, who will inform the relevant NextGen Project task lead at Mathematica. Mathematica’s incident response team will follow the NextGen/ACF incident response procedures to investigate the issue.

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 system includes several features to ensure the integrity, availability, accuracy, and relevance of PII in the system.

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: Data is stored in the cloud, available 24/7, and accessible from multiple platforms.

Accuracy and Relevancy: Key fields must be completed to proceed with a task. Where applicable, fields have edit checks to ensure that data is 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. Mathematica also completes routine reviews of the data to ensure accuracy and relevancy. For example, Mathematica project staff confirm that the address fields 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.

The most restrictive set of access rights/privileges needed to perform specified tasks in the system is enforced. Least privilege for specified system roles is applied in accordance with risk assessments to adequately mitigate risk to PII.

Access to the NextGen Project system will be limited to only a few Mathematica task leads on the NextGen Project and system developers.

Programs being evaluated will specify which program staff require access permission based on business need. The Mathematica task lead will then assign program users to appropriate roles.

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 access privileges are implemented in RAPTER and the SMS. Users are assigned to specific roles. Each role is limited to specific access privileges based on their needs. Mathematica task leads define these roles and the associated access privileges when establishing program user accounts.

Access privileges are assigned using the concept of least privilege for specified duties.

Data is segregated by program sites. Program staff users do not have access to data in other sites.

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.

Mathematica staff, including NextGen SMS users, receive annual security awareness training that addresses the security policies and procedures contained in the Mathematica Security Manual. All staff must review and acknowledge Mathematica's Rules of Behavior. Staff sign confidentiality pledges that stipulate sanctions for non-compliance and complete Mathematica’s online security awareness training shortly after their start date. Refresher training is delivered annually thereafter to remind staff of the relevant sanctions.

Programs receive training on the proper use of RAPTER and the procedures they must follow to protect the PII contained in the system. They also receive periodic follow-ups stressing important

secure system and data handling practices.

All personnel including both direct contractors and government personnel are required to participate in the ACF annual security compliance training and privacy training.

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

The NextGen Project team will conduct trainings with all staff who may have access to sensitive information, including Mathematica staff and staff from the programs in the study. All study staff with access to PII will receive study-specific training on (1) limitations on disclosure; (2) safeguarding the physical work environment;(3) storing, transmitting, and destroying data securely; and (4) reporting on potential data breaches or incidents that adhere to ACF and HHS requirements. The project team will conduct additional trainings for staff (including program study staff) that are responsible for data that are relevant to their specific data collection roles. For example, data collectors will also be trained on ensuring that participants will be able to answer questions in a safe and secure manner. All procedures will be documented in study-specific training manuals that will be developed in advance of data collection and updated as needed. Refresher trainings will occur as needed between the annual refresh cycle.

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 records containing PII are temporary and will be destroyed 3 years after cutoff. Cutoff occurs when the records become obsolete, are superseded, or are no longer needed to support program activities.

The records retention schedule for these records is 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.

To secure PII, the NextGen Project system leverages the security capabilities of Amazon Web Services (AWS) FedRAMP services and applications, and the policies and procedures that have been implemented for the Mathematica enterprise and specifically for the NextGen Project.

Administrative controls include policies and procedures around protection of PII. These include NextGen Project system training, system procurement, separation of duties and least privilege, security planning, change control, and auditing. They also include complying with concepts of only collecting the minimum PII necessary to conduct the NextGen Project and following directives concerning non-disclosure of PII.

Technical controls include the hundreds of automated capabilities that enforce access permissions to PII, encryption of PII in transit and at rest, password and multifactor authentication requirements, audit logging/monitoring/alerting, network intrusion and prevention, protection against malware, separation of duties, and least privilege.

Physical controls, including those provided by AWS, include facility security procedures such as protecting against unauthorized access to, loss of, and theft of PII, as well as procedures to protect the people who work on the NextGen Project and its related project systems.