US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/06/2016

OPDIV:

ACF

Name:

Research and Evaluation Studies

PIA Unique Identifier:
P-7740519-898352

The subject of this PIA is which of the following?
Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.
Operations and Maintenance

Is this a FISMA-Reportable system?
No

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)?
No

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

Describe the purpose of the system.
The systems covered by this PIA support the following HHS Strategic Goals: Goal 2: Advance Scientific Knowledge and Innovation; Goal 3: Advance the Health, Safety, and Well-Being of the American People; and Goal 4: Ensure Efficiency, Transparency, Accountability, and Effectiveness of HHS Programs. The systems also support ACF's goal to upgrade the capacity of ACF to make a difference for families and communities.

In collaboration with ACF program offices and others, OPRE is responsible for performance management for ACF, conducts research and policy analyses, and develops and oversees research and evaluation projects to assess program performance and inform policy and practice. The procedures for the collection of information about research subjects in OPRE's evaluation projects are reviewed, as appropriate, by the Office of Management and Budget and Institutional Review Boards, and are subject to HHS regulations on research with human subjects, including requirements for informed consent.

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

Records in this system may be about any individual who participates in an ACF/OPRE-sponsored research demonstration. The specific types of records collected and maintained are determined by the needs of each research and evaluation project. Typical projects will collect some or all of these records: name; address; telephone number and other contact information; Social Security Number (SSN); demographic information, including race and ethnicity; date of birth; income; pre-school/Head Start participation; child care utilization; marriage and family status information; health information; income; employment information; child welfare system experiences; citizenship, etc. Information collected will be used to assess program performance and inform policy and practice. Submission of personal information is voluntary.

This data may be directly entered into the system by the system end user or may be derived from interface or upload from another information technology system or database. The system may interface with another information technology system or database to transfer already-collected data to the research contractor. As detailed in individual contracts with those collecting data, all data transfer is completed in compliance with Department of Health and Human Services standards, including National Institute of Standards and Technology (NIST) and Federal Information Processing Standard (FIPS). Information is not shared outside of the system. All data is accessed by end users through authorized and access-controlled user accounts. Users of the system include ACF contractors, researchers, employees, and grantees. Information collected to establish accounts and access control may include name, email address and phone number.

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

The specific types of records collected and maintained are determined by the needs of each research and evaluation project. Typical projects will collect some or all of these records: name; address; telephone number and other contact information; Social Security Number (SSN); demographic information, including race and ethnicity; date of birth; income; pre-school/Head Start participation; child care utilization; marriage and family status information; health information; income; employment information; child welfare system experiences; citizenship, etc. Information collected will be used to assess program performance and inform policy and practice. Submission of personal information is voluntary.

PII is shared within HHS and with Other Federal Agency/Agencies and State or Local Agency/Agencies, and the private sector for data matching purposes. Users of the system include ACF contractors, researchers, employees, and grantees. Information collected to establish accounts and access control may include name, email address and phone number.

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

Biometric Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Financial Accounts Info

Certificates

Legal Documents

Education Records

Military Status

Employment Status

race; ethnicity; citizenship; income

pre-school / Head Start participation

child welfare system experiences

marriage and family status information

user credentials

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?

100,000-999,999

For what primary purpose is the PII used?

OPRE conducts research and policy analyses, and develops and oversees research and evaluation projects to assess program performance and inform policy and practice for ACF. Individual’s PII is often necessary for research and policy analyses. The PII is essential for establishing association between and among various data sets and elements used for research and policy analysis.

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

Research and policy development, including end user account creation and access control.

Describe the function of the SSN.

The SSN is used to match with administrative records.

Cite the legal authority to use the SSN.

Social Security Act, SEC. 1110: Cooperative Research or Demonstration Projects; Social Security Act, Sec. 413; Social Security Act, Sec 2008 as enacted by Sec 5507 of the Affordable Care Act; Improving Head Start for School Readiness Act of 2007, Sec 641(c)(2) and Sec 649; Child Care and Development Block Grant Act of 1990, as amended, and Consolidated Appropriations Act of 2010; Social Security Act, Sec. 429; Foster Care Independence Act of 1999; Keeping Children and Families Safe Act of 2003; Social Security Act, Sec 426; Affordable Care Act, Sec 2951; Deficit Reduction Act of 2005, and subsequent TANF extensions; Social Security Act, Sec 403(a)(2) as amended by the Welfare Integrity and Data Improvement Act of FY12.

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

Social Security Act: Section 1110; Section 413; Section 429; Section 2008 (as enacted by Section 5507 of the Affordable Care Act); and Section 403(a)(2) (as amended by the Welfare Integrity and Data Improvement Act of FY12).

Improving Head Start for School Readiness Act of 2007: Section 649 and Section 641 (c)(2)

Child Care and Development Block Grant Act of 1990, as amended

Consolidated Appropriations Act of 2010

Affordable Care Act: Section 2951

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

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Other Federal Entities

Other

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Whenever the Paperwork Reduction Act (PRA) is implicated, we will obtain an Office of Management and Budget (OMB) information collection approval number and expiration date.
Current OMB information collections include:
0970-0151 (Exp 03/31/2019)
0970-0355 (Exp 03/15/2018)
0970-0356 (Exp 03/15/2018)
0970-0373 (Exp 09/30/2016)
0970-0394 (Exp 12/31/2017)
0970-0397 (Exp 12/31/2017)
0970-0398 (Exp 11/31/2017)
0970-0402 (Exp 08/31/2018)
0970-0403 (Exp 12/31/2016)
0970-0408 (Exp 07/31/2017)

0970-0413 (Exp 09/30/2017)
0970-0414 (Exp 11/30/2018)
0970-0440 (Exp 02/28/2018)
0970-0460 (Exp 07/31/2018)
0970-0462 (Exp 08/31/2018)
0970-0468 (Exp 12/31/2016)
0970-0469 (Exp 12/31/2017)
0970-0470 (Exp 12/31/2016)
0970-0471 (Exp 12/31/2017)
0970-0472 (Exp 01/31/2018)
0970-0479 (Exp 04/30/2017)
0970-0481 (Exp 07/31/2019)
0970-0487 (Exp 09/30/2019)

Additional approvals are pending and/or expected in the future.

Is the PII shared with other organizations?

Yes

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

Within HHS

Only for data matching purposes

Other Federal Agencies

Only for data matching purposes

State or Local Agencies

Only for data matching purposes

Private Sector

Only for data matching purposes

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

PII may be shared for research purposes under strict privacy procedures or shared as required by law.

The system may interface with another information technology system for data and information exchange. In such cases, the research contractor has or will establish a Computer Matching Agreements (CMA) as required. Data is accessed by end users through authorized and access controlled user accounts. Information is not shared outside of the system. No disclosure or sharing of PII is permitted or performed that is not governed by a formal agreement.

Describe the procedures for accounting for disclosures.

Disclosures are governed by agreements that detail the data to be shared, the IT security standards, the people authorized to use the data, and the purpose and limitations on use. Any unauthorized disclosures must be reported within 24 hours. Any disclosure of PII outside of the system will be addressed in collaboration with the HHS Privacy Incident Response Team (PIRT), according to the PIRT standard operating procedures. A response plan will be developed and implemented, through this process, we will document the date, nature, and purpose of each disclosure; and the name and address of the recipient. These records will be maintained for a period of five years after the disclosure occurred or the life of the record (whichever is longer).

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

Respondents will be provided with information about how their PII will be used and will be informed that responses are voluntary. All collections including PII will require consent from respondents. Consent forms will notify individuals that their personal information will be collected. System administrators complete a first time user registration process for account creation and will be notified that their user credentials will be created at that time and stored/collected within the system.

Information collections requesting PII will inform individuals about the information collected from them through a consent process, either verbal or written, which describes both the information to be requested and the use of such information. Information collected will be analyzed and reported in aggregate; participants will not be identified in public domain unless they have consented to be identified. PII may be shared for research purposes under strict privacy procedures or shared as required by law.

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.

Respondents will be informed that their participation is voluntary and they may choose to not participate in the study or to skip questions within the data collection. This information will be included within consent forms and data collection instructions. Potential system administrators will be informed that their participation is voluntary and they may decline to complete a user profile.

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

A verbal or written consent is obtained as part of the data collection process. Through the consent process, individuals will receive clear and comprehensive information about the use of their information. Information collected will be analyzed and reported in aggregate; participants will not be identified in public documents unless they have consented to be identified. PII may be shared for research purposes under strict privacy procedures or shared as required by law. If PII will be used for any materially different purposes other than proposed in an original consent, updated consent will be requested.

The system administrator notifies end users with PII in the system and their consent is obtained when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection).

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.

Information collected will be analyzed and reported in aggregate; participants will not be identified in public documents unless they have consented to be identified. PII may be shared for research purposes under strict privacy procedures or shared as required by law. As required by the Paperwork Reduction Act, information collection materials include information about who to contact at the research contractor for questions or concerns.

The following PII data is collected from end users for access control: name, e-mail address, location (mailing address) and phone number and is based upon consent of the end users for creating an end user account. There are processes 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. System users contact the system program manager or system help desk with concerns about their user account.

An investigation will be completed to: identify any potential unauthorized access, improper use of data, policy violations; data breaches; data thefts; malicious code; loss or stolen equipment; characterize the type and extent of any potential PII involved; and conduct a risk assessment fordetermination of the potential risk exposure. Once the investigation is completed corrective actions and countermeasures will be developed, a determination made, and actions taken to address the potential loss or theft of PII. Corrective actions could include: training and awareness; implementation of new and revised policies; review and expansion of existing technologies or implementation of new technologies; or strengthening or hardening existing safeguards and security.

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

Requirements, policies and guidelines regarding retention and destruction of the PII are specified in the contracts for those collecting and storing data.

Contractors will maintain back-up servers to ensure PII is not improperly or inadvertently modified or destroyed. System users are asked to review and update their information on a regular basis to ensure that it is accurate and up-to-date. In general, for research that is longitudinal, respondents will be asked to confirm or update contact information. Data Integrity is maintained through user access recertification and encryption for data at rest and in transit.

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

Users:

Business purposes.

Administrators:

System management

Contractors:

For Business purposes. A list of contractor sites where records under this system are maintained is available upon request to the system manager.

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

All contractors or other record keepers are required to maintain appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. End user accounts are created and maintained by research contractors who review, authorize and approve the creation of the end user account based upon the individual end user’s roles and responsibilities associated with the specific Research and Evaluation Studies project. End user roles and responsibilities will determine the type and content data and information necessary for job function (both PII and Non-PII). Role-based access will determine and control who will have access to PII. The authorized and approved account creation request is submitted to the system administrator who creates the individual account and notifies the end user of the authorized, approved, and created account.

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.

End user accounts are created and maintained by research contractors who review, authorize and approve the creation of the end user account based upon the individual end user’s roles and responsibilities associated with the specific ACF Research and Evaluation Studies project. End user roles and responsibilities will determine the type and content data and information necessary for job function (both PII and Non-PII). Role-based access will determine and control who will have access to PII. The authorized and approved account creation request is submitted to the system administrator who creates the individual account and notifies the end user of the authorized, approved, and created account.

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 project staff undergoes security awareness training and review the procedures for handling PII on the project. In addition, project staff, grantee staff, and ACF staff sign a confidentiality form before access to the system or the data can be granted. ACF employees will complete any mandatory training. Examples of these trainings include Annual HHS Information Systems Security Awareness Training; Annual HHS Privacy Training; and Reading the Rules of Behavior for Use of HHS Information Resources and signing the accompanying acknowledgment.

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

Contractors shall ensure that all of its employees, subcontractors (at all tiers), and employees of each subcontractor, who perform work under this contract/subcontract, are trained on data privacy issues and comply with the Federal and Departmental regulations for private 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.

Depending on the project, records may be stored on paper or other hard copy, computers, and networks. Identifiers are stored separately from survey data and removed once analysis is complete. All contractors or other record keepers are required to maintain appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. Records are secured in compliance with Federal requirements, including the Federal Information Security Management Act, HHS Security Program Policy, and any applicable requirements for the encryption of personal data.

OPRE is in communications with the ACF Records Manager to determine the specific National Archives and Records Administration (NARA) retention schedule. All records will be retained until a determination is made as to the final records disposition schedule. Once established the records will be disposed consistent with the records disposition schedule.

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

PII is secured using the following:

Administrative controls, such as:
System security plan (SSP)
File backup/archive conducted by hosting agency (NIHCIT)
User manuals
Contractor Agreements

Technical Controls, such as:
User Identification and Authorization
Passwords
Firewalls at hosting site and Department firewall for federal staff computers
Monitoring and Control scans provided by hosting agency
PIV cards

Physical controls, such as:
The system servers are hosted in a secure data center and can be physically accessed by only authorized infrastructure staff

Enforcement of established physical security capabilities (management walk-throughs and assessment of security locks, doors, desks, storage materials), Security Guards employing access controls to individuals requesting facility access: Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
All physical access to data centers by employees is logged and audited routinely.

Physical containment and isolation of Systems, Data bases, and Storage assets that collection, maintain, store, and share PII

Secured and limited access facilities: data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee.

Compartmentalization and physical separation of system components (servers, cables, storage access, off-site backup facilities and storage)