

**U.S. Department of Housing and
Urban Development**

**Office of Policy Development and
Research**

Family Self-Sufficiency Program Demonstration Data

Privacy Impact Assessment

March 12, 2013

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **[Insert Name of IT System and/ or Information Collection Request]**. This document has been completed in accordance with the requirement set forth by the [E-Government Act of 2002](#) and [OMB Memorandum 03-22](#) which requires that "Privacy Impact Assessments" (PIAs) be conducted for all new and/ or significantly altered IT Systems, and Information Collection Requests.

ENDORSEMENT SECTION

Please check the appropriate statement.

- The document is accepted.**
 The document is accepted pending the changes noted.
 The document is not accepted.

Based on our authority and judgment, the data captured in this document is current and accurate.

/s/ Jennifer Stoloff, Program Evaluation Division

SYSTEM OWNER

Office of Policy Development and Research

3/13/2013

Date

/s/ Carol Star, Division Director, Program Evaluation

PROGRAM AREA MANAGER

Office of Policy Development and Research

3/13/2-13

Date

/s/ Donna Robinson-Staton

DEPARTMENTAL PRIVACY ACT OFFICER

Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

3/13/2013

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	2
TABLE OF CONTENTS	3
SECTION 1: BACKGROUND.....	4
Importance of Privacy Protection – Legislative Mandates:	4
What is the Privacy Impact Assessment (PIA) Process?	5
Who Completes the PIA?.....	5
When is a Privacy Impact Assessment (PIA) Required?.....	5
What are the Privacy Act Requirements?	6
Why is the PIA Summary Made Publicly Available?	6
SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT	7
Question 2: Type of electronic system or information collection.....	11
Question 3: Explain by Line of Business why the personally identifiable information being collected? How will it be used?	12
Question 4: Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module or outside the government)?.....	14
Question 5: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?.....	14
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	15
Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?.....	16
Question 9: What are the Retention Use and Disposal Practices. Guidance for this section should obtain from HUD retention use and disposal policy. It should also be validated that these procedures are outlined in the contracted service agreement to ensure that the contracted system does not hold onto data after services are no longer provided.....	17
SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER.....	18

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
FAMILY SELF-SUFFICIENCY DEMONSTRATION DATA**

March 12, 2013

NOTE: See Section 2 for PIA answers, and Section 3 for Privacy Act Officer's determination.

SECTION 1: BACKGROUND

Importance of Privacy Protection – Legislative Mandates:

HUD is responsible for ensuring the privacy and confidentiality of the information it collects on members of the public, beneficiaries of HUD programs, business partners, and its own employees. These people have a right to expect that HUD will collect, maintain, use, and disseminate identifiable personal information only as authorized by law and as necessary to carry out agency responsibilities.

The information HUD collects is protected by the following legislation and regulations:

- [Privacy Act of 1974, as amended](#) affords individuals the right to privacy in records that are maintained and used by Federal agencies. (See <http://www.usdoj.gov/foia/privstat.htm>; see also [HUD Handbook 1325.1 at www.hudclips.org](#));
- Computer Matching and Privacy Protection Act of 1988 is an amendment to the Privacy Act that specifies the conditions under which private information may (or may not) be shared among government agencies. (See <http://www.usdoj.gov/foia/privstat.htm>);
- [Freedom of Information Act of 1966, as amended](#) (http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm) provides for the disclosure of information maintained by Federal agencies to the public, while allowing limited protections for privacy. See also [HUD's Freedom of Information Act Handbook \(HUD Handbook 1327.1 at www.hudclips.org\)](#));
- [E-Government Act of 2002](#) requires Federal agencies to conduct Privacy Impact Assessments (PIAs) on its electronic systems. (See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf; see also the summary of the E-Government Act at http://www.whitehouse.gov/omb/egov/pres_state2.htm);
- [Federal Information Security Management Act of 2002](#) (which superceded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security regulations at [Title 44 U.S. Code chapter 35 subchapter II](#) (<http://uscode.house.gov/search/criteria.php>); and

- [OMB Circular A-130, Management of Federal Information Resources, Appendix I \(http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf\)](http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) defines Federal Agency responsibilities for maintaining records about individuals.

Access to personally identifiable information will be restricted to those staff that has a need to access the data to carry out their duties; and they will be held accountable for ensuring privacy and confidentiality of the data.

What is the Privacy Impact Assessment (PIA) Process?

The Privacy Impact Assessment (PIA) is a process that evaluates issues related to the privacy of personally identifiable information in electronic systems. See background on PIAs and the 7 questions that need to be answered, at: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>. Personally identifiable information is defined as information that actually identifies an individual, e.g., name, address, social security number (SSN), or identifying number or code; or other personal/ sensitive information such as race, marital status, financial information, home telephone number, personal e-mail address, etc. Of particular concern is the combination of multiple identifying elements. For example, knowing name + SSN + birth date + financial information would pose more risk to privacy than just name + SSN alone.

The PIA:

- Identifies the type of personally identifiable information in the system (including any ability to combine multiple identifying elements on an individual);
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to HUD's mission is included.

Who Completes the PIA?

Both the program area System Owner and IT Project Leader work together to complete the PIA. The System Owner describes what personal data types are collected, how the data is used, and who has access to the personal data. The IT Project Leader describes whether technical implementation of the System Owner's requirements presents any risks to privacy, and what controls are in place to restrict access of personally identifiable information.

When is a Privacy Impact Assessment (PIA) Required?

- 1. New Systems:** Any new system that will contain personal information on members of the public requires a PIA, per OMB requirements (this covers both major and non-major systems).
- 2. Existing Systems:** Where there are significant modifications involving personal information on members of the public, or where significant changes been made to the system that may create a new privacy risk, a PIA is required.

3. Information Collection Requests, per the Paperwork Reduction Act (PRA):

Agencies must obtain OMB approval for new information collections from ten or more members of the public. If the information collection is both a new collection and automated, then a PIA is required.

What are the Privacy Act Requirements?

Privacy Act. The Privacy Act of 1974, as amended (<http://www.usdoj.gov/foia/privstat.htm>) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The E-Government Act of 2002 requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Why is the PIA Summary Made Publicly Available?

The E-Government Act of 2002 requires that the analysis and determinations resulting from the PIA be made publicly available. The Privacy Advocate in HUD's Office of the Chief Information Officer (OCIO) is responsible for publishing the PIA summary on HUD's web site. See: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>.

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Please submit answers to the Departmental Privacy Act Officer in the Office of the Chief Information Officer (OCIO). If any question does not apply, state Not Applicable (N/A) for that question, and briefly explain why it is not applicable.

Program Area: Office of Policy Development & Research, Program Evaluation Division
Subject Matter Expert in the Program Area: Jennifer Stoloff, GTR / Elizabeth Rudd, GTM
Program Area Manager: Carol Star, Division Director
IT Project Leader: N/A. This is not an IT system.

For IT Systems: **N/A. This is not an IT system.**

- **Name of system:**
- **PCAS #:**
- **OMB Unique Project Identifier #:**
- **System Code:**
- **Development Date:**
- **Expected Production Date:**

For Information Collection Requests:

- **Name of Information Collection Request:** Family Self-Sufficiency Demonstration Data
- **OMB Control #:** Not yet available; this is a new information collection.

Question 1: Provide a general description of the system. The following questions are intended to define the scope of the information in the system (or information collection), specifically the nature of the information and the sources from which it is obtained.

- a. What is the personal information being collected?**
- b. From whom is the information collected (i.e., government employees, contractors, or consultants)?**

It will be collected from participants in the Family Self-Sufficiency Demonstration and from administrative data sets that contain information about participants in the Family Self-Sufficiency Demonstration. Data elements and sources are listed below.

- Collected at the time of random assignment through data entry in MDRC's random assignment application from self-reporting by study participants and/or data entry of HUD 50058 or other administrative data retrieved by program staff. Study participant's:
 - Social Security Number
 - Full name
 - Date of birth
 - Public Housing Authority Household ID number
 - Address

- Phone numbers
- Email addresses
- Contact information of family or friends (to facilitate locating the study participant for follow-up survey interviews).
- Extracted after random assignment through matches to statewide, county, or local administrative records systems
 - Employment and education and training MIS ID number, if one or more Management Information Systems is developed. (Note: MIS ID may be a randomly-generated ID number created by MDRC)
 - Public assistance Case Number
 - Public assistance PersonID Number
 - Unemployment Insurance Wage State- or Federal Employer ID Numbers

Non-PII Identifiers

MDRC will create 2 internal-use randomly-generated ID numbers:

- SampleID: never shared with providers or the survey firm
- RESID (ResearchID): Pre-printed on participant Informed Consent Forms and Contact Information forms and shared with pre-employment and education and training services providers and with survey firm

Participant and household characteristics

- Collected at the time of random assignment through data entry in MDRC's random assignment application from self-reporting by study participants
 - Gender
 - Race/ethnicity
 - Educational attainment
 - Marital status
 - Number of adults and children in household
 - Current and prior employment
 - Employment of other household members
 - Household income
- Extracted from HUD 50058 form or other HUD administrative data around the time of random assignment through match by PHA Household ID number
 - Family structure (relationship codes)
 - Number in household
 - Type of action
 - Effective date of action
 - Household assets (aggregated by Household ID number)
 - Household Income (aggregated by Household ID number)
 - Income Code
 - Dollars per Year

- Income After Exclusions
 - Adjusted Annual Income
 - Total Tenant Payment
 - Subsidy amount
- Extracted after random assignment through matches to statewide, county, or local administrative records systems
 - Pre-random assignment employment and earnings from quarterly UI Wage data
 - Pre-random assignment SNAP/food stamps and TANF receipt

POST-RANDOM ASSIGNMENT PROGRAM OUTCOMES

- Extracted from HUD 50058 form or other HUD administrative data through matches by PHA Household ID number
 - Family structure (relationship codes)
 - Number in household
 - Type of action
 - Effective date of action
 - Household assets (aggregated by Household ID number)
 - Household Income (aggregated by Household ID number)
 - Income Code
 - Dollars per Year
 - Income After Exclusions
 - Adjusted Annual Income
 - Total Tenant Payment
 - Subsidy amount
 - Eligibility status for the FSS escrow account
 - Contributions to FSS escrow account (dates and amounts)
 - Withdrawals from FSS escrow account (dates and amounts)
 - Eligibility status for Section 8 housing
 - [If applicable:] Residence status in public housing
 - [If applicable:] Participation in other HUD programs or use of financial incentives (for example, Earned Income Disregard for public housing residents)
- Extracted through matches to Management Information Systems of FSS pre-employment and education and training services providers
 - Service type
 - Service referral, start, and end dates
 - End reason (completed, on hold, withdrew...)
 - Degree/credential receipt
 - Supportive services payment type, date received, and amount
- Extracted through matches to statewide, county, or local administrative records systems
 - Employment and earnings from quarterly UI Wage data

- Unemployment Insurance Benefit receipt and benefit amounts
- SNAP/food stamps and TANF receipt and benefit amounts
- Collected from responses to follow-up survey(s).
 - Experiences with and participant assessment of the FSS program
 - Understanding of and agreement/disagreement with program requirements
 - Reasons for exit
 - Plans for/Use of money in escrow account
 - Experiences with other public housing programs
 - Degree/credential receipt
 - Use of education and training or employment services
 - Dates of employment and job characteristics
 - Respondent and household income
 - Material hardship
 - Family well-being
 - Savings, debt, and financial behaviors
 - Household demographics
 - Housing circumstances and conditions

c. What is the functionality of the system and the purpose that the records and/or system serve?

This information collection, known as the Family Self Sufficiency Program Demonstration, will produce a dataset to be used to study the Family Self-Sufficiency program and evaluate the impacts on individuals and households of participation in the Family Self Sufficiency program. The Family Self Sufficiency Program Demonstration is a project of the HUD Transformation Initiative authorized by Congress. The data will enable HUD to assess whether participants in FSS are more likely to become self-sufficient because of participating in the program.

d. How is information transmitted to and from the system?

Baseline and survey data will be collected through phone interviews. Administrative data will be collected through a secure system in which the contractor, MDRC, will create request files with only needed identifiers for matching to agency administrative data. The request files will be sent using secure procedures, either electronically or by courier; the matched data files will be returned to MDRC using secure procedures either electronically or by courier.

e. What are the interconnections with other systems.

N/A. This is not an IT system. This information collection will result in a research dataset.

- f. **What specific legal authorities, arrangement, and/or agreement authorize the collection of information (i.e. must include authorities that cover all information collection activities, including Social Security Numbers)?**

Section 502 (g) of the Housing and Urban Development Act of 1970 (Public Law 91-609) (12 U.S.C. 1701z-1; 1701z-2(d) and (g)).

Question 2: Type of electronic system or information collection.

This is an information collection, therefore items A, B, and C are N/A.

	Yes	No
A. If a new electronic system (or one in development) (implemented after April 2003, the effective date of the E-Government Act of 2002)?	<input type="checkbox"/>	X <input type="checkbox"/>
Does the system require authentication?	<input type="checkbox"/>	<input type="checkbox"/>
Is the system browser-based?	<input type="checkbox"/>	<input type="checkbox"/>
Is the system external-facing (with external users that require authentication)?	<input type="checkbox"/>	<input type="checkbox"/>

B. If this is existing electronic system has the system undergone any changes (since April 17, 2003)? If an existing system, when was the system developed? _____	Yes	No
Do the changes to the system involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?	<input type="checkbox"/>	<input type="checkbox"/>
If yes, please explain:		

C. For your new and/or existing electronic system, please indicate if any of the following changes have occurred: Mark any of the following conditions for your existing system that OMB defines as a “trigger” for requiring a PIA or PIA update (if not applicable, mark N/A):	
	Conversion: When paper-based records that contain personal information are converted to an electronic system
	From Anonymous (Non-Identifiable) to “Non-Anonymous” (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
	Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new “relational” databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when

	a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)
	Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)
	New Public Access: When <u>new</u> public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology)
	Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)
	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data
	Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)

D. If an Information Collection Request (ICR): Is this a <u>new</u> Request that will collect data that will be in an <u>automated</u> system? Agencies must obtain OMB approval for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a <u>new</u> request and the collected data will be in an <u>automated</u> system.	
XX	Yes, this is a new ICR and the data will be automated
	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>)
	Comment:

Question 3: Explain by Line of Business why the personally identifiable information is being collected? How will it be used?

Mark any that apply:

Homeownership:

	Credit checks (eligibility for loans)
	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
	Loan default tracking

	Issuing mortgage and loan insurance
	Other (specify):

Rental Housing Assistance:

	Eligibility for rental assistance or other HUD program benefits
	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
	Property inspections
	Other (specify):
	Comment:

Grants:

	Grant application scoring and selection – if any personal information on the grantee is included
	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
	Comment:

Fair Housing:

	Housing discrimination complaints and resulting case files
	Other (specify):
	Comment:

Internal operations:

	Employee payroll or personnel records
	Payment for employee travel expenses
	Payment for services or products (to contractors) – if any personal information on the payee is included
	Computer security files – with personal information in the database, collected in order to grant user IDs
	Other (specify):
	Comment:

Other lines of business (specify uses): RESEARCH AND EVALUATION

X	<p>Comment: PII is required in order to construct a data set that includes both responses to survey items and data extracted from administrative agencies for the same individuals. This is necessary in order to assess the impact of participating in the FSS program on participants' self-sufficiency.</p> <p>Data collected for this study will be used only for research and evaluation purposes. It will never be used for any other purpose. Study participants will be informed of their rights and that their information will be kept private. The study will require the permission of an institutional review board that protects the rights of human subjects.</p>
---	---

Question 4: Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module or outside the government)?

Mark any that apply:

	Federal agencies?
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	HUD module/application? (specify the module(s)/application(s) name)
X	Others? (specify): State unemployment insurance systems and possibly other administrative agencies; a very small number of authorized researchers who work for the contractor (MDRC) and possibly with researchers awarded cooperative agreements under the Fiscal Year 2012 Transformation Initiative: Family Self Sufficiency Program Demonstration Small Grant Research Program.
X	Comment: PII will be shared with authorized researchers and with administrative agencies in limited ways and only for the specific purpose of constructing data sets required to conduct research and evaluation studies. Authorized researchers will be employees of MDRC, the contractor conducting the Family Self Sufficiency Demonstration and recipients of grant awards (cooperative agreements) under the <i>Fiscal Year 2012 Transformation Initiative: Family Self Sufficiency Program Demonstration Small Grant Research Program</i> . Any such disclosures will occur only after execution of written agreements that specify purpose, terms and conditions of sharing HUD data, including compliance with the Privacy Act of 1974 and demonstrating adequate data security systems. Data analysis for research and evaluation will be conducted using a de-identified data set.

Question 5: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?

XX	Yes, they can “opt-out” by declining to provide private information or by consenting only to particular use.
	No, they can’t “opt-out” – all personal information is required

	Comment:
--	----------

If Yes, please explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

**PARTICIPATION IN THE RESEARCH STUDY IS VOLUNTARY.
RESPONDENTS ARE NOT REQUIRED TO PROVIDE ANY INFORMATION
THAT THEY DO NOT WISH TO PROVIDE.**

**Question 6: How will the privacy of the information be protected/ secured?
What are the administrative and technological controls?**

Please see the attached discussion of data security and quality control.

Mark any that apply and give details if requested:

X	System users must log-in with a password (Please specify password type): MDRC computers use fingerprint scanning. In addition, MDRC uses a strong password system that requires passwords to be at least 8 characters, use a combination of capital- and lower-case letters, numbers, and special characters. MDRC employees are forbidden to share passwords. Passwords are stored encrypted, not displayed when entered. Passwords expire every month. Three unsuccessful logins lead to locking access to the network. An application associates each employee's fingerprint with his/her network password.
X	When an employee leaves: <ul style="list-style-type: none"> • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? <ul style="list-style-type: none"> ▪ Departing employees' computer account and access rights are disabled at the close of business on their last day of employment. • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): <ul style="list-style-type: none"> ▪ Technical controls determine that departing employees no longer have access to the system.
X	Are access rights selectively granted, depending on duties and need-to-know? Yes, access rights are selectively granted, depending on duties and need-to-know. If Yes, specify the approximate # of authorized users who have either: <ul style="list-style-type: none"> • Full access rights to all data in the system: 2 • Limited/restricted access rights to only selected data: 19
X	Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe your plan to improve): Data is stored in MDRC's Data Center. It has been designed and built in accordance with local building and fire codes. Access to the room is available via two doors which each require a properly authorized swipe card

	for access. Card access is recorded 24 hours per day, every day. The doors may also be locked by means of a physically embedded lock mechanism requiring a key. Anyone approaching the doors of the adjacent corridor is recorded by camera. Internal network racks which house infrastructure, security and encryption equipment are locked, front and back.
X	If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to improve: MDRC will not release PII to reside in another data system. MDRC will not share FSS Demonstration data except (1) sharing of de-identified data sets with authorized researchers and (2) sharing of a minimum amount of personal identifying information with researchers awarded cooperative agreements under HUD's <i>Fiscal Year 2012 Transformation Initiative: Family Self Sufficiency Program Demonstration Small Grant Research Program</i> . Such researchers will be required to comply with the Privacy Act of 1974 and demonstrate adequate data security procedures.
X	Other methods of protecting privacy (specify): MDRC has a comprehensive set of technical, physical, and corporate controls to ensure the protection of PII possessed by the firm. Please see the attached document, "MDRC's Data Security Technologies and Protocols."
	Comment:
	Privacy Impact Analysis: Given the access and security controls, what privacy risks were identified and describe how they were mitigated.

Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?

Mark any that apply

	Name:
X	Social Security Number (SSN)
X	Identification number (specify type), possibilities include: Public Assistance Case number, Public assistance PersonID number, Unemployment Insurance Wage State- or Federal Employer ID Numbers, SampleID, RESID, PHA Household ID number
X	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
X	Home address
	Home telephone
	Personal e-mail address
X	Other (specify): PHA Household ID number
	None

X	<p>Comment:</p> <p>This is not an IT system. The privacy information will be retrieved from the data set in very limited circumstances for very limited purposes: (1) to extract data about study participants from administrative data sets and (2) to support the completion of research projects awarded cooperative agreements under HUD’s Fiscal Year 2012 Family Self Sufficiency Small Grant Research Program.</p> <p>For matching with administrative records several of the listed elements might be used in order to maximize accuracy of the match.</p> <p>Data analysis will be conducted with a de-identified dataset.</p>

Question 8: What type of Notice(s) are provided to the individual on the scope of information collected, the opportunity to consent to uses of said information, the opportunity to decline to provide information.

- a. Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on form(s), and/or a system of records notice published in the Federal Register.) If notice was not published, why not?**

A SORN will be published. The draft SORN is attached.
 Informed consent procedures will be implemented.

- b. Do individuals have an opportunity and/or right to decline to provide information?**

Participation in the FSS Demonstration is voluntary. Individuals have the right to decline to participate in general and the right to drop out of the study at any point in time.

- c. Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?**

Study participants are informed of their rights as research subjects through procedures approved by MDRC’s institutional review board (IRB). Please see the attached document, “MDRC’s Data Security Technologies and Protocols” for information on MDRC’s IRB.

Question 9: What are the Retention Use and Disposal Practices? Guidance for this section should obtain from HUD retention use and disposal policy. It should also be validated that these procedures are outlined in the contracted

service agreement to ensure that the contracted system does not hold onto data after services are no longer provided.

a. How long is information retained?

MDRC will destroy all electronic and paper records with PII by the end date of the FSS contract unless otherwise instructed by HUD. Per MDRC's standard procedure, the Data Librarian and project Data Manager will verify that all incoming files are accounted for at the end of the project—deleted or permanently archived, per agreement with HUD and with data providers.

b. Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

YES

Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Please see the attached document, "MDRC's Data Security Technologies and Protocols" for information on MDRC's IRB.

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER

The Office of Privacy has reviewed the PIA and has determined that there are proper security and privacy controls in place to protect the data from improper use and disclosure. PD&R will revisit the PIA prior to deploying the ICR to make subsequent changes resulting from new functionality and/or business requirement, if necessary.