

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

Office of Policy Development & Research

Rapid Re-housing for Homeless Families Data Files

Privacy Impact Assessment

July 8, 2010

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for the **Rapid Re-housing for Homeless Families Data Files**. 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.



**SYSTEM OWNER, ANNE FLETCHER
OFFICE OF POLICY DEVELOPMENT &
RESEARCH**

11/3/10
Date



**PROGRAM AREA MANAGER, CAROL STAR
DIRECTOR, PROGRAM EVALUATION
DIVISION**

11/3/10
Date

DEPARTMENTAL PRIVACY ACT OFFICER
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	2
ENDORSEMENT SECTION	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 1: Provide a brief description of what personal information is collected.....	7
Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?	9
Question 3: Type of electronic system or information collection.....	11
Question 4: Why is the personally identifiable information being collected? How will it be used?	13
Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?	15
Question 6: 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)?.....	15
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	16
Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?.....	18
SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER.....	19

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:**

RAPID RE-HOUSING FOR HOMELESS FAMILIES DATA FILES

JULY 8, 2010

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 **Error! Hyperlink reference not valid.**);
- 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) 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: Program Evaluation Division, RRE, Office of Policy Development & Research
Subject matter expert in the program area: Anne L. Fletcher, Office of Policy Development and Research, Program Evaluation Division, (202) 402-4347

Program Area Manager: Carol S. Star, Office of Policy Development and Research, Program Evaluation Division, (202) 402-6139

IT Project Leader: N/A, not an internal HUD system so no IT Project Leader

For IT Systems:

- **Name of system:** Rapid Re-housing for Homeless Families Data Files
- **PCAS #:** N/A
- **OMB Unique Project Identifier #:** N/A
- **System Code:**
- **Development Date:**
- **Expected Production Date:**

For Information Collection Requests:

- **Name of Information Collection Request:** Evaluation of the Rapid Re-housing for Homeless Families Demonstration Program
- **OMB Control #:** TBD

Question 1: Provide a general description of the system that describes:

The FY 2008 budget for the U.S. Department of Housing and Urban Development (H.R. 2764) included a \$25 million set-aside to implement a Rapid Re-housing for Families Demonstration Program “expressly for the purposes of providing housing and services to homeless families.” In order to measure the efficacy of the program, HUD will seek to enroll approximately 1,200 participating families into an outcomes evaluation. Participant contact data will be collected upon entry into the program, and a follow-up survey will be administered to each participating family twelve months after completion of the program. The survey will collect data related to housing stability; self-sufficiency; employment and earnings; family well-being; and health.

The Rapid Re-housing for Homeless Families Data Files will include data from roughly 1,200 families who choose to participate in the evaluation, including: participant contact information; data collected through the initial family assessment and the 12-month follow-up survey;; data collected from third parties for tracking purposes; and data about study families that are collected from existing administrative databases such as the local Homeless Management Information System (HMIS). Confidentiality of personal identifying information (PII) collected for this

study will be maintained through a combination of management, operational, and technical controls, which are defined broadly in NIST SP 800-53, and are the basis of HUD's policies as defined in HUD Information Technology Security Policy, Handbook 2400.25 Rev. 1. The privacy and security protocols will address the three core principles of information security: confidentiality, availability and integrity. Please see Appendix A for a full description of the Data Security Plan pertaining to the Rapid Re-housing for Homeless Families Data Files.

If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then mark any of the categories that apply below:

Personal Identifiers:

X	Name
X	Social Security Number (SSN). Specify the purpose/legal authority authorizing the solicitation of SSNs (This includes truncated SSNs): SSNs are required to match the participant study records with other already existing administrative data sets for purposes of locating participants for the 18-month follow-up survey and for assessing client outcomes in a broad range of domains.
X	Other identification number (specify type): Participant Study ID #: This ID # will be a randomly generated unique ID that will allow the research team to link identifiers with study files.
X	Birth date
X	Home address
X	Home telephone
X	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None
	Comment:

Personal/ Sensitive Information:

X	Race/ ethnicity
X	Gender/ sex
X	Marital status
X	Spouse name
X	# of children
X	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.): Earned income, benefit receipt (e.g. SSI, SSDI, TANF, etc.)
X	Employment history:
X	Education level
X	Medical history/ information
X	Disability

X	Criminal record
X	Other (specify): Exposure to violence; homeless program utilization, barriers to housing
	None
	Comment:

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?

	Yes	No
If yes, Proceed to answering the following questions.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Have the security controls been reviewed and approved by the Information Security Officer?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

What security controls are in place to protect the information (e.g., encryptions)?

Physical safeguards during Transmission

All personal data (identifiable and de-identified data analyses files) will be encrypted and maintained on a secure workstation or server that is protected by a firewall, complex passwords, and multi-authentication factors, in a directory that can only be accessed by the network administrators and the analysts actively working on the data. Data on the secure server will be encrypted using an industry standard algorithm incorporating at least 128-bit encryption. The decryption key will only be known to analysts actively working with the data. Separate data files will be maintained for each questionnaire and for identifying information. Data files used for analysis will be stored in a separate location from files with identifying information to minimize the risk that an unauthorized user could use the unique identification number to link de-identified files with the identifiers. The unique identification number will be protected through multi-mode authentication, in addition to encryption technologies. Access rights to the data are granted to limited researchers on a need-to-know basis, and the level of access provided to each researcher is based on the minimal level required that individual to fulfill his research role. Abt Associates will backup the data on a regular basis to safeguard against system failures or disasters. Only encrypted versions of the data will be copied to the backup media. Unencrypted data will never be stored on a laptop or on a movable media such as CDs, diskettes, or USB flash drives. If an authorized researcher leaves employment or is no longer working on this project, their user ID and access will be terminated within one day, as will VPN access. These steps will be documented as part of termination process. The site interviewers will securely store any hard copy documents with personal protected information, such as signed consent forms, tracking letters, or interview appointment schedules.

The participation agreement/informed consent and contact information form will be a paper form. After the family signs the informed consent form, the RRHD program staff person will record the participant's contact information in the secure, web-based study contact database. After the contact information is recorded, the hardcopy form will be placed within a sealed envelope and stored temporarily in a locked cabinet in a secure physical location within the RRHD program's administrative office. (If the contact information cannot be immediately recorded in the database, the RRHD program staff will store the signed form in the designated locked cabinet until the staff person is able to record the data. Alternatively, the program can submit the signed form to the Abt Director of Analysis, and Abt research staff can enter the contact information into the study contact database.)

The site interviewer will store any tracking letters, appointment schedules, or other documentation with personal protected information, such as name, in a locked cabinet that can only be accessed by the interviewer. Tracking documentation with personal protected information should not be generated until needed in the tracking process to limit risk of unauthorized disclosures. Site interviewers should use study IDs in lieu of personal protected information on tracking documentation whenever feasible to limit risk of unauthorized disclosures. All hard copy forms with personal identifying data (the participant agreement/informed consent form) will be stored securely in a locked cabinet that can only be accessed by authorized individuals working on the data. The locked cabinet will be stored in a locked office in a limited access building.

What HUD approved application is used to grant remote access (e.g., VPN, Citrix)? VPN

Is there a policy in place restricting remote access from certain locations outside the Department (For example: Policy may permit remote access, but prohibits access from a particular place; such as, Kinko's/Starbucks) or is remote access permitted from all areas outside the Department? Remote access from particular locations is not expressly prohibited within the security plan; however, authorized users are required to ensure that identifiable data will only be accessed in appropriate and secure physical locations. Access is only planned from within Abt's office locations or secure offices of its subcontractors or consultants. Access is only permitted on approved Abt or AbtSRBI equipment.

Is there a policy that identifies "if" or "if not" downloading and remote storage of this information is allowed (For example: Policy may permit remote access, but prohibit downloading and local storage)? Policy does not prohibit downloading or locally storing the data; however, data may only be accessed on approved Abt or AbtSRBI equipment and data stored on a mobile device or laptop must be stored in an encrypted format.

Comment:

Question 3: Type of electronic system or information collection.

	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 checked="" type="checkbox"/>	<input type="checkbox"/>
Does the system require authentication? Complex password, multi-factor authentication.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system browser-based? The general study database will not be browser-based; however, some data will be collected through the study's contact database website and compiled within a secure	<input checked="" type="checkbox"/>	<input type="checkbox"/>

system that is not browser-based.		
Is the system external-facing (with external users that require authentication)?	<input checked="" 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
	<input type="checkbox"/>	<input checked="" type="checkbox"/>
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"/>
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.	
X	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 4: Explain by Line of Business why the personally identifiable information is being collected? How will it be used?

The FY 2008 budget for the U.S. Department of Housing and Urban Development (H.R. 2764) included a \$25 million set-aside to implement a Rapid Re-housing for Families Demonstration Program “expressly for the purposes of providing housing and services to homeless families.” Also included in the legislation was a requirement that there be an evaluation of the demonstration program “in order to evaluate the effectiveness of the rapid re-housing approach in addressing the needs of homeless families.” The Notice of Funding Availability (NOFA) issued by HUD stated that “the Rapid Re-housing Demonstration program will include an evaluation phase, which will focus on determining the efficacy of the assessment process and the housing/service intervention related to how successfully households are able to independently sustain housing after receiving short-term leasing assistance.” In order to measure the effectiveness of the program, it will be necessary to follow families after program completion and ascertain if there have been any improvements along the measures that we are seeking to impact, such as housing stability; self-sufficiency; employment and earnings; family well-being; and health.

Contact information for each family that chooses to participate in the evaluation will be collected at the time of program enrollment and periodically updated throughout program enrollment, as well as six months following exit from the program, in order to maintain contact with each family to facilitate the follow up survey at a later date. The follow-up survey, to be conducted 12 months after program exit, will be used to measure outcomes for participating families in several domains, including:

housing stability; self-sufficiency; employment and earnings; family well-being; and health.

The study will involve collecting personal information from families enrolled in the study at the time of study enrollment, and twelve months after the conclusion of the receipt of assistance. Procedures are being put in place to ensure confidentiality of data and records both from a data management and survey administration perspective. Personal information will not be collected from study participants without first obtaining written consent. Thereafter, the information will be secured through a combination of management, operational, and technical controls, which are defined broadly in NIST SP 800-53, and are the basis of HUD’s policies as defined in HUD Information Technology Security Policy, Handbook 2400.25 Rev. 1.

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):
	Comment:

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:

X	Grant application scoring and selection – if any personal information on the grantee is included
X	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):

x	Research data compilation and analysis

Question 5: 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)
	Others? (specify):
	Comment:

Question 6: 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)?

X	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 study and completion of any aspect of the survey are 100% voluntary. There are no risks that families participating in the study will lose benefits they might otherwise receive. Further, families are free to opt out of the study at any point for any reason with no negative repercussions. Alternatively, not participating in the study will not pose any risks of losing other benefits to which the family might otherwise be eligible.

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

Mark any that apply and give details if requested:

X	System users must log-in with a password (Please specify password type): complex password and multi-factor authentication for remote access by authorized research personnel
X	When an employee leaves: <ul style="list-style-type: none"> • How soon is the user ID terminated? 1 day (1 day, 1 week, 1 month, unknown)? • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): As part of employee termination process, user IDs are terminated, VPN access is terminated, the authentication keyfob must be returned, and an employee termination worksheet documenting these steps is completed.
X	Are access rights selectively granted, depending on duties and need-to-know? Yes. 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: Approximately 3 Limited/restricted access rights to only selected data: <ul style="list-style-type: none"> ▪ Approximately 3 AbtSRBI researchers with access to data collected directly from participating families across all sites. ▪ Approximately 5 AbtSRBI researchers with access to data collected directly from participating families in the site in which he/she is collecting data; that is, each of these individuals will only have access to the data in one site. ▪ Approximately 5 Abt researchers with access to de-identified individual-level data. <p>Each data user's permissions will be defined based on the user's role on the project. For example, the local site interviewer will be able to review data for study participants only for his or her own specific site. Only a very small number of researchers will have access to the complete identifiable dataset</p>
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): Yes. The site interviewers will securely store any hard copy documents with

	<p>personal protected information, such as signed consent forms, tracking letters, or interview appointment schedules.</p> <p><i>Consent Forms.</i> The participation agreement/informed consent and contact information form will be a paper form. After the family signs the informed consent form, the RRHD program staff person will record the participant's contact information in the secure, web-based study contact database. After the contact information is recorded, the hardcopy form will be placed within a sealed envelope and stored temporarily in a locked cabinet in a secure physical location within the RRHD program's administrative office. (If the contact information cannot be immediately recorded in the database, the RRHD program staff will store the signed form in the designated locked cabinet until the staff person is able to record the data. Alternatively, the program can submit the signed form to the Abt Director of Analysis, and Abt research staff can enter the contact information into the study contact database.)</p> <p><i>Tracking documentation.</i> The site interviewer will store any tracking letters, appointment schedules, or other documentation with personal protected information, such as name, in a locked cabinet that can only be accessed by the interviewer. Tracking documentation with personal protected information should not be generated until needed in the tracking process to limit risk of unauthorized disclosures. Site interviewers should use study IDs in lieu of personal protected information on tracking documentation whenever feasible to limit risk of unauthorized disclosures. All hard copy forms with personal identifying data (the participant agreement/informed consent form) will be stored securely in a locked cabinet that can only be accessed by authorized individuals working on the data. The locked cabinet will be stored in a locked office in a limited access building. Hard copy forms that are no longer needed for the study will be shredded. If site interviewers do not have access to a paper shredder, they will submit the paperwork to the Abt Director of Analysis via FedEx with clear instructions to destroy the documents upon receipt.</p>
	<p>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:</p> <p>Not applicable; data will not be shared with another system or data warehouse.</p>

X	<p>Other methods of protecting privacy (specify):</p> <p>All personal data (identifiable and de-identified data analyses files) will be encrypted and maintained on a secure workstation or server that is protected by a firewall, complex passwords, and multi-authentication factors, in a directory that can only be accessed by the network administrators and the analysts actively working on the data. Data on the secure server will be encrypted using an industry standard algorithm incorporating at least 128-bit encryption. The decryption key will only be known to analysts actively working with the data.</p> <p>Separate data files will be maintained for each questionnaire and for identifying information. Data files used for analysis will be stored in a separate location from files with identifying information to minimize the risk that an unauthorized user could use the unique identification number to link de-identified files with the identifiers. The unique identification number will be protected through multi-mode authentication, in addition to encryption technologies.</p> <p>Abt Associates will backup the data on a regular basis to safeguard against system failures or disasters. Only encrypted versions of the data will be copied to the backup media. Unencrypted data will never be stored on a laptop or on a movable media such as CDs, diskettes, or USB flash drives.</p>
	Comment:

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

Mark any that apply

X	Name:
X	Social Security Number (SSN)
X	Identification number (specify type):
X	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
	None
	Comment:

Is there an existing Privacy Act System of Records Notice (SORN) that has been published in the Federal Register to cover this system? Yes No (Please consult with your component's Privacy office if assistance is needed in responding to this question.)

The Privacy Act System of Records Notice (SORN) has been developed in draft and is pending publication.

If yes, provide the Federal Register citation

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER