

U.S. Department of Housing and Urban Development

Office of Housing

Home Equity Reverse Mortgage Information Technology (HERMIT)

Privacy Impact Assessment

December 13, 2012

HERMIT Privacy Impact Assessment

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for Home Equity Reverse Mortgage Information Technology (HERMIT). 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/ William F. Fuentevilla

SYSTEM OWNER;

William F Fuentevilla

Office of Housing Finance and Budget

8/24/12

Date

/s/ William F. Fuentevilla

PROGRAM AREA MANAGER;

William F Fuentevilla

Office of Housing Finance and Budget

8/24/12

Date

12/19/2012

/s/ Donna Robinson-Staton

DEPARTMENTAL PRIVACY ACT OFFICER;

Donna Robinson-Staton

Office of the Chief Information Officer

U. S. Department of Housing and Urban Development

Date

HERMIT Privacy Impact Assessment

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT 2
ENDORSEMENT SECTION 2
PLEASE CHECK THE APPROPRIATE STATEMENT..... 2
THE DOCUMENT IS ACCEPTED..... 2
THE DOCUMENT IS ACCEPTED PENDING THE CHANGES NOTED..... 2
THE DOCUMENT IS NOT ACCEPTED..... 2
SYSTEM OWNER; 2
PROGRAM AREA MANAGER;..... 2
DEPARTMENTAL PRIVACY ACT OFFICER; DONNA ROBINSON-STATON..... 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 general description of the system that describes: 7
 Question 2: Type of electronic system or information collection..... 10
 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)?..... 13
 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?..... 14
 Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?..... 15
 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. 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..... 16
SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER..... 18

HERMIT Privacy Impact Assessment

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

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 superseded 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.

HERMIT Privacy Impact Assessment

Access to personally identifiable information will be restricted to staff members who have 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) evaluates issues related to the privacy of personally identifiable information in electronic systems. See the background on PIAs and the seven 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 for 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?

The program area system owner and IT project leader collaborate to complete the PIA. The system owner describes what types of personal data 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 to personally identifiable information.

When is a Privacy Impact Assessment (PIA) Required?

- 1. New Systems:** Any new system that will contain personal information about 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 about 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.

HERMIT Privacy Impact Assessment

What are the Privacy Act Requirements?

Privacy Act. The [Privacy Act of 1974](http://www.usdoj.gov/foia/privstat.htm), 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>.

HERMIT Privacy Impact Assessment

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Subject matter experts in the program area:

Sally M. Bene, National Servicing Center
Eric A. Davidson, Single Family Housing
Shawn. A. Ford, Finance and Budget
Robert J. Gould, Single Family Housing
Erica L. Jessup, Single Family Housing
Richard Nkamanyi, Finance and Budget
Lisa A. Simms, National Servicing Center
Josephine Huang, Office of Evaluation

Program Area Manager: William F. Fuentevilla

IT Project Leader: William F. Fuentevilla

For IT Systems:

- **Name of system:** Home Equity Reverse Mortgage Information Technology (HERMIT)
- **PCAS #:** N/A - Not using Working Capital Funds
- **OMB Unique Project Identifier #:** N/A
- **System Code:** P271
- **Development Date:** November 1, 2009 – October 2012
- **Expected Production Date:** October 9, 2012

For Information Collection Requests:

Name of Information Collection Request: N/A

HERMIT functionality is not accessible by the general public, but only by authorized users.

- **OMB Control #:** N/A

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

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? (e.g. name, address, gender/sex, race/ethnicity, income/financial data, employment history, medical history, Social Security Number, Tax Identification Number, Employee Identification Number, FHA Case Number).**

The personal information collected by the system is the name, home address and telephone number, date of birth, Social Security Numbers, tax identification number (TIN), ABA Routing Number (For Servicers).

HERMIT Privacy Impact Assessment

b. From whom is the information collected (i.e., government employees, contractors, or consultants)? Information is collected

From HECM mortgagees by HECM mortgagors for Home Equity Conversion Mortgages insured under HUD's HECM mortgage insurance program. FHA collects the information from the HECM mortgagors through other HUD systems. These other HUD systems, in turn, transmit the information to HERMIT. HERMIT does not collect the information directly.

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

HERMIT provides FHA with comprehensive solution that integrates and/or automates the five processes that encompass the HECM program (insurance servicing; claim payments; notes servicing; accounting, and reporting). HERMIT is based on a specialized commercial off-the-shelf (COTS) product from Reverse Mortgage Services (RMS) that meets the requirements needed to service reverse mortgages for the HECM program. The system collects, stores, presents, and delivers core reverse mortgage data, including all borrower and loan characteristics. The service performs various services such as loan boarding, accruals, loan transaction processing, compliance monitoring, and default management.

HERMIT relies on other HUD systems that process the HECM mortgage insurance applications and to underwrite and endorse HECM cases.

HERMIT uses an off-the-shelf financial package from Savantage for the accounting needs of reverse mortgage processing. HERMIT obtains, stores, and tracks accounting events and displays financial information regarding HECM Premiums, Claims, Notes and foreclosed properties acquired by or in custody of HUD. HERMIT supports accounting operations to ensure that FHA's financial management functions meet Federal requirements for tracking budgetary resources and controlling funds. All accounting processes comply with Financial Systems Integration Office (FSIO – formerly Joint Financial Management Improvement Program – JFMIP) and Federal Credit Reform Act standards. HECM SP provides support for accounts payable, payment, accounts receivable, billing, collection and budgetary accounting and control functions associated with FHA HECM management and associated contract services; and processes HECM collections and disbursements via Treasury, commercial bank, or other (Lockboxes and Pay.gov, etc.) systems. HERMIT exchanges data with a number of HUD and non-HUD systems, including the existing CHUMS and FHA Subsidiary Ledger on a daily basis.

HERMIT Privacy Impact Assessment

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

The information about endorsed loans that FHA is adding to the HECM insurance-in-force portfolio, including the personal information identified under Question 1a, is transmitted to HERMIT from the Computerized Homes Underwriting Management System (CHUMS). HERMIT’s interfaces with other HUD systems are depicted below in Figure 1, HERMIT System Interfaces.

e. What are the interconnections with other systems?

The HERMIT system interacts with several HUD legacy and external systems. The following diagram (Figure 1) displays the various systems that interact with HERMIT and the types of users who will be accessing it. The interfaces are file-based, and the files are exchanged using SFTP.

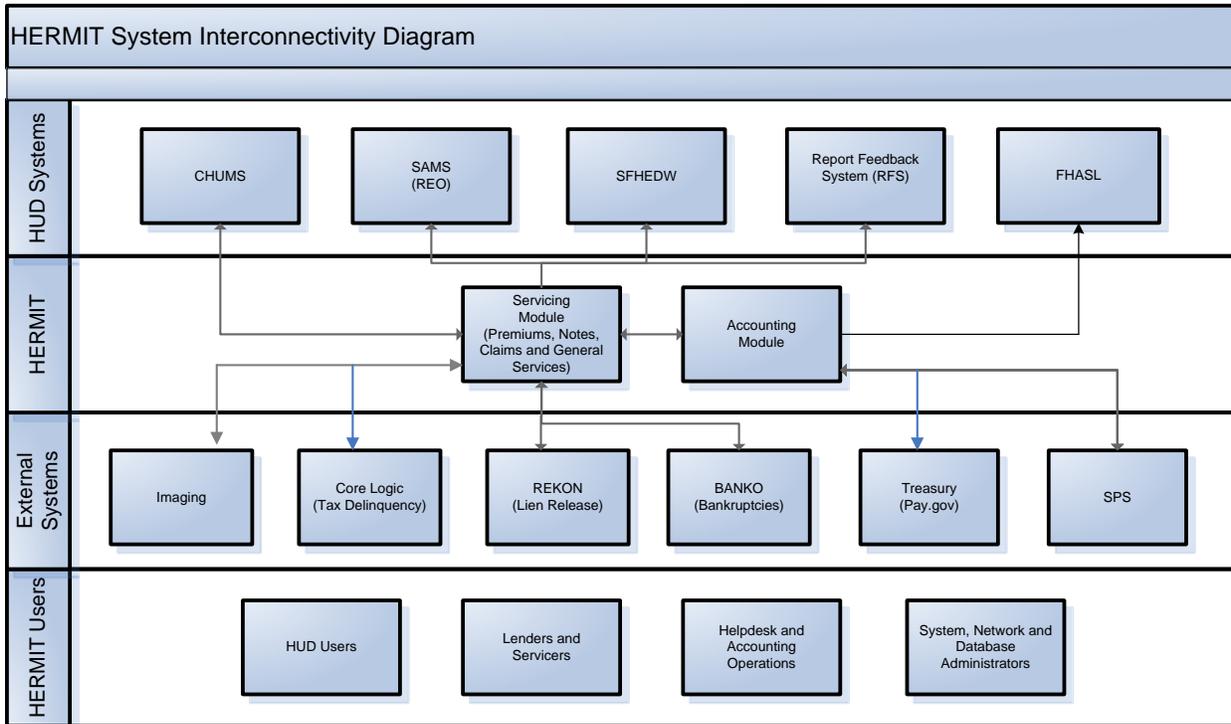


Figure 1: HERMIT – System Interfaces

HERMIT Privacy Impact Assessment

- 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)?**

The National Housing Act of 1934 authorizes the FHA reverse mortgage program for the elderly, the Home Equity Conversion Mortgage (HECM) program (12 U.S.C.1715Z-20).

The Housing and Community Development Act of 1987 (42 U.S.C. 3543 - Sec. 3543) specifically provides authority to collect Social Security Numbers:

(a) Disclosure of social security account number. As a condition of initial or continuing eligibility for participation in any program of the Department of Housing and Urban Development involving loans, grants, interest or rental assistance of any kind, or mortgage or loan insurance, and to ensure that the level of benefits provided under such programs is proper, the Secretary of Housing and Urban Development may require that an applicant or participant (including members of the household of an applicant or participant) disclose his or her social security account number or employer identification number to the Secretary.

(b) Definitions For purposes of this section, the terms "applicant" and "participant" shall have such meanings as the Secretary of Housing and Urban Development by regulation shall prescribe. Such terms shall not include persons whose involvement is only in their official capacity, such as State or local government officials or officers of lending institutions.

Question 2: 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?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system browser-based?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system external-facing (with external users that require authentication)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

HERMIT Privacy Impact Assessment

B. If this is existing electronic system has the system undergone any changes (since April 17, 2003)?	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 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 checked="" 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:	
	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
X	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)
X	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)
X	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)
X	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)

HERMIT Privacy Impact Assessment

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.	
	Yes, this is a new ICR and the data will be automated
X	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 being collected? How will it be used?

Homeownership:

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

Rental Housing Assistance: N/A

	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:N/A

	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:N/A

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

HERMIT Privacy Impact Assessment

Internal Operations: N/A

	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):N/A

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)?

<input checked="" type="checkbox"/>	Federal agencies? US Treasury
<input checked="" type="checkbox"/>	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
<input checked="" type="checkbox"/>	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
<input checked="" type="checkbox"/>	HUD module/application? (specify the module(s)/application(s) name) <ul style="list-style-type: none"> • CHUMS • SFHEDW • SAMS • GINNIE MAE • REKON • FARETS • BANKO • IMAGING • PAY.GOV • SPS • FHASL
	Others? (specify):
	Comment:

HERMIT Privacy Impact Assessment

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)?

	Yes, they can “opt-out” by declining to provide private information or by consenting only to particular use
X	No, they can’t “opt-out” – all personal information is required
	Comment: Since HERMIT receives personal information from CHUMS and not from individuals directly, this question does not apply to HERMIT system.

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): _____

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

X	System users must log-in with a password (Please specify password type) HUD employees and approved lenders/servicers must use individually assigned user IDs and passwords to access HERMIT. The password must be changed immediately. Security features include: A minimum of 8 alpha-numeric characters (with at least one number or special character included), no requirements for CAPS. Account gets auto-locked if there is no activity within 90 days. User account never gets deleted, but only gets disabled.
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)? <p>The HERMIT system administrator terminates User IDs in accordance with HERMIT’s account management procedures. System access is deactivated within <u>1 day</u> of notification by the user’s project manager.</p> <ul style="list-style-type: none"> • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): <p>Once a user is deactivated by the HERMIT system administrator, the user is denied access to the system. The application administrator can check the status of the user by logging on to the application and reviewing the User Search screen. HERMIT also automatically deactivates any user if there are no activities by the user within the 90-day period.</p>
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either:

HERMIT Privacy Impact Assessment

	<ul style="list-style-type: none"> • Full access rights to all data in the system: 1 HUD System/Application Administrator • Limited/restricted access rights to only selected data: Less than 500 users
X	<p>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):</p> <ul style="list-style-type: none"> • Yes, the disks, tapes and printouts that contain personal information are locked in cabinets.
	<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>ICDs are in place between shared systems. The ICDs are used as the primary means of protecting the privacy of the data being shared with the other system.</p> <p>Refer to the Security section in the ICD for protection specifics.</p>
	Other methods of protecting privacy (specify):
	Comment:

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

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

HERMIT Privacy Impact Assessment

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?**

The system will publish a System of Records Notice (SORN) prior to production.

Borrower personal information is received from CHUMS and is not editable in HERMIT.

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

N/A to HERMIT since information is sourced from CHUMS. Individuals don't provide input to HERMIT directly.

- 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?**

N/A to HERMIT since information is sourced from CHUMS. Individuals don't provide input to HERMIT directly.

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?**

Retention and Disposal: Records are held in accordance with HUD's Records Disposition Schedules Handbook (2225.6) Appendix 20. Paper Records are not in use. All electronic data is kept indefinitely and not deleted. Archival Tape Media is kept for 7 years and the Tapes are in rotation. Tapes that are faulty and need to be disposed of follow the NIST 800-88 guidelines section 2.1.

HERMIT Privacy Impact Assessment

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

Retention and Disposal: Records are held in accordance with HUD's Records Disposition Schedules Handbook (2225.6) Appendix 20. Paper Records are not in use. All electronic data is kept indefinitely and not deleted. Archival Tape Media is kept for 7 years and the Tapes are in rotation. Tapes that are faulty and need to be disposed of follow the NIST 800-88 guidelines section 2.1.

HERMIT Privacy Impact Assessment

SECTION 3 - DETERMINATION BY HUD PRIVACY ACT OFFICER

The Privacy Impact Assessment for HERMIT is approved.