

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

Office of Housing

Hospital Mortgage Insurance Management
Information System - - HMIMIS

Privacy Impact Assessment

May 2005

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for Hospital Mortgage Insurance Management Information System. 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.

MANAGEMENT ENDORSEMENT

Please check the appropriate statement.

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

/s/ Eric M. Stout

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

Dec. 15, 2005

Date

/s/ Jeanette Smith

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

Dec. 15, 2005

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 1: Provide a brief description of what information is collected.	7
Question 2: Type of electronic system or information collection.....	9
Question 3: Why is the personally identifiable information being collected? How will it be used?	10
Question 4: Will you share the information with others?	11
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)?	12
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	12
Question 7: If private information is involved, by what data elements can it be retrieved? .	13
SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE	13

DRAFT

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
“HOSPITAL MORTGAGE INSURANCE
MANAGEMENT INFORMATION SYSTEM - HMIMIS”
(OMB Unique Identifier N/A and PCAS # 00251560)
May 2, 2005**

NOTE: See Section 2 for PIA answers, and Section 3 for Privacy Advocate’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 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) (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 HUD staff who have been authorized because of their duties; and they will be held accountable for ensuring privacy and confidentiality.

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](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>.

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Please submit answers to the Departmental Privacy Advocate 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 Housing/ Office of Insured Health Care Facilities, HUD

Subject matter expert in the program area: John Whitehead, Director, Insured Health Care Facilities, Office of Housing, HUD, (202) 708-0599 Ext 5790,

Program area manager: John Whitehead (see above)

IT Project Leader: Dorothy H. Mitchell, Information Technology System Integration and Efficiency, Office of the Chief Information Officer, HUD, 708-0517, ext 7496; Thomas Williams, Chicago Operation Branch, Office of Administration, HUD, 708-0517, ext. 6069

For IT Systems:

- **Name of system:** Hospital Mortgage Insurance Management Information System - HMIMIS
- **PCAS #:** 00251560
- **OMB Unique Project Identifier # (if submitting an Exhibit 300 to OMB):** N/A (not a major system, therefore an Exhibit 300 was not submitted to OMB)

For Information Collection Requests:

- **Name of Information Collection Request:**
- **OMB Control #:**

Question 1: Provide a brief description of what information is collected.

HMIMIS provides the Office of Housing with the information that HUD needs to conduct careful underwriting and monitoring to avoiding claims in its Section 242 hospital mortgage insurance programs, which tend to be very large and visible projects. The system is used by HUD and shared with the Department of Health and Human Services (HHS) to perform underwriting and monitoring functions through the vehicle of an interagency agreement.

To avoid the possibility of financial risks in hospital mortgages, HUD and HHS managers evaluate statistical data to detect early warning signs of potential problems of hospitals to prevent hospitals from getting into serious financial difficulty. The system streamlined the processes of old automated and paper systems into a one-stop shop affording managers the opportunity to analyze the full scope of the project at a program or specific hospital level. Specifically, HMIMIS will analyze the:

- Financial performance of portfolio hospitals;
- Quality of financial feasibility studies;
- Portfolio characteristics;
- Risk Management; and track
- Performance measures, etc.

The information in the systems consists of data from the audited financial statements of hospitals with HUD-insured loans, details of each loan from HUD's F-47 system, and various data pertaining to the loan origination and loan management processes performed by HUD and

HHS staff. However, the stakeholders may consider the financial data contained in the system confidential and would not welcome release to some parties such as competitors, the media, unions engaged in negotiations with hospitals.

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:

<input checked="" type="checkbox"/>	Name
<input type="checkbox"/>	Social Security Number (SSN)
<input type="checkbox"/>	Other identification number (specify type):
<input type="checkbox"/>	Birth date
<input type="checkbox"/>	Home address
<input checked="" type="checkbox"/>	Home telephone
<input type="checkbox"/>	Personal e-mail address
<input type="checkbox"/>	Fingerprint/ other "biometric"
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	None
<input type="checkbox"/>	Comment: The only information collected on HUD employees is their name and phone number for business purposes. Only the name and home phone number of HUD and HHS employees, which cannot be sorted to retrieve personal identifiers/ sensitive information of that employee. The home phone number is optional and is only used to contact HUD employees who are working from home.

Personal/ Sensitive Information:

<input type="checkbox"/>	Race/ ethnicity
<input type="checkbox"/>	Gender/ sex
<input type="checkbox"/>	Marital status
<input type="checkbox"/>	Spouse name
<input type="checkbox"/>	# of children
<input type="checkbox"/>	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
<input type="checkbox"/>	Employment history
<input type="checkbox"/>	Education level
<input type="checkbox"/>	Medical history/ information
<input type="checkbox"/>	Disability
<input type="checkbox"/>	Criminal record
<input type="checkbox"/>	Other (specify):
<input checked="" type="checkbox"/>	None
<input checked="" type="checkbox"/>	Comment: HMIMIS evaluates the financial status of hospitals insured by HUD, but does <u>not</u> collect <u>nor</u> does it contain personally identifiable information on the hospital.

Question 2: Type of electronic system or information collection.

Fill out Section A, B, or C as applicable.

A. If a new electronic system (or one in development): Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?

	Yes
X	No

B. If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a “trigger” for requiring a PIA (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)
X	N/A (Specify) Not a major system, therefore an Exhibit 300 was not submitted to OMB

C. If an Information Collection Request (ICR): Is this a new Request that will collect data that will be in an automated 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 new request and the collected data will be in an automated system.

<input type="checkbox"/>	Yes, this is a new ICR and the data will be automated
<input type="checkbox"/>	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>)
<input type="checkbox"/>	Comment:

Question 3: Why is the personally identifiable information being collected? How will it be used?

Mark any that apply:

Homeownership:

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

Rental Housing Assistance:

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

Grants:

<input type="checkbox"/>	Grant application scoring and selection – if any personal information on the grantee is included
<input type="checkbox"/>	Disbursement of funds to grantees – if any personal information is included
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	Comment:

Fair Housing:

<input type="checkbox"/>	Housing discrimination complaints and resulting case files
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	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
X	Other (specify): HMIMS evaluates the financial status of hospitals insured by HUD, but does <u>not</u> collect <u>nor</u> does it contain personal identifiable information on the hospital.
	Comment:

Other lines of business (specify uses):

Other related information pertaining to the Department (please specify):

	Other (specify):
	Comment:

Question 4: Will you share the information with others?

For Example, another agency for a programmatic purpose, or outside the government.

Mark any that apply:

X	Federal agencies? (specify): The Department of Health and Human Services (HHS)
	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?
	Others? (specify):
	Comment:.

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
	No, they can’t “opt-out” – all personal information is required
X	Comment: <u>N/A, Employees can opt-out of providing home phone numbers</u>

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?

Mark any that apply and give details if requested:

X	System users must log-in with a password (Note: via a user name and password that must be approved and issued by the office of Insured Health Care Facilities).
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)? <u>Usually 1 month after termination</u> • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve):
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the # of authorized users who have either: <ul style="list-style-type: none"> • Full access rights to all data in the system (specify #)? <u>About 30 individuals to ensure that no data is added to or removed from the system erroneously. Audit trails and journaling – N/A due to low sensitivity of system data.</u> • Limited/ restricted access rights to only selected data (specify #)?
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): <u>N/A only reports. N/A, Not a privacy concern, the report printout is only of the business contact, which includes their name and business number for business purposes.</u>
	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:

	Other methods of protecting privacy (specify):
	Comment:

Question 7: If private information is involved, by what data elements can it be retrieved?

Mark any that apply:

<input checked="" type="checkbox"/>	Name
	Social Security Number (SSN)
	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
<input checked="" type="checkbox"/>	Home telephone
	Personal e-mail address
	Other (specify):
	None
	Comment:

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY HUD PRIVACY ADVOCATE

HMIMIS is not a concern for privacy protection, personally identifiable information is not entered into the tool nor does it collect privacy information on hospitals insured by HUD. The system is only available to about thirty individuals, by job function via an access code that must be approved and issued by the office of Insured Health Care Facilities. Only the home phone # of a small number of HUD and HHS users of the system is collected, and that is optional (they can opt-out).