FEDERAL HOUSING FINANCE AGENCY

Use and Protection of Personally Identifiable Information Policy

Approved: Edward J. DeMarco **Date:** 8/22/2010

Edward J. DeMarco, Acting Director

Title: Use and Protection of Personally Identifiable Information Policy

TABLE OF CONTENTS

Title: Use and Protection of Personally Identifiable Information Policy

I. PURPOSE

To establish the Federal Housing Finance Agency's (FHFA) policy on the collection, use, maintenance, and security of personally identifiable information (PII).

II. SCOPE

This policy applies to all FHFA employees, contractor personnel, and personnel from other entities (entity personnel) that have legal access to information maintained by FHFA (e.g., FHFA Office of Inspector General, Government Accountability Office, and Office of Personnel Management). The requirements pertain to all electronic systems and paper files that collect, store, process and/or maintain PII.

III. POLICY

The Privacy Act of 1974 requires Federal agencies to establish appropriate administrative, technical, and physical safeguards to protect records from threats which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained. The sections below outline specific requirements for protecting PII.

A. Collecting, Using, and Maintaining PII. PII must be collected and used in accordance with FHFA policy, guidance, procedures, and applicable System of Records Notice (SORN). FHFA employees, contractor personnel, and entity personnel must:

1. Be able to identify PII material in their possession and take appropriate safeguards to protect it;

2. Avoid the unnecessary collection and maintenance of sensitive PII, especially social security numbers;

3. Restrict access to only those people who need the PII to perform their official duties;

4. Report any known or suspected breaches to the Chief Privacy Officer (CPO) in accordance with the FHFA Breach Notification Policy and Plan;

5. Complete annual privacy training and education; and

6. Properly dispose of PII when it is no longer needed.

B. Sharing PII. PII records may be shared only if authorized by law or with the express written consent of the affected individual. Sharing is limited to the portion of the

record necessary to complete the task requested. Before sharing PII outside of FHFA, an employee, contractor personnel, or entity personnel must contact the CPO to ensure such sharing complies with applicable privacy laws and FHFA privacy policies, except for disclosures of records for law enforcement purposes or information made by the Office of Inspector General to the Department of Justice, or to a chair of a committee for either House of Congress and its committees and subcommittees to the extent the information pertains to matters within their jurisdiction and with FHFA's receipt of a written request from the committee chair.

C. **New Data Collection.** Before collecting data that includes PII, employees, contractor personnel, or entity personnel must consult the CPO to ensure that privacy requirements have been satisfied.

D. **Consequences.** Failure to comply with this policy may result in disciplinary action up to and including termination from the federal service. Further, violating the Privacy Act may result in criminal and/or civil penalties.

IV. DEFINITIONS

A. **Individual,** for purposes of the Privacy Act, is a citizen of the United States or an alien lawfully admitted for permanent residence. The Privacy Act does not apply to non-resident aliens, deceased individuals, or organizations.

B. **PII** is information that can be used to distinguish or trace an individual's identity, such as name, home address, telephone number, social security number, or biometric records, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date of birth or mother's maiden name.

C. **Record,** for purposes of the Privacy Act, is any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, criminal or employment history, and that contains the individual's name, or identifying number, symbol, or other particular assigned to the individual, such as a finger print, voice print, or photograph.

D. **Sensitive PII** is a subset of PII that if released would pose a higher risk of subsequent identity theft or personal harm. For example, a Social Security number is sensitive PII. Sensitive PII also includes an individual's name, home address, or telephone number in combination with any of the following:

1. Government-issued identification number, such as a driver's license number;

2. Date or place of birth;

3. Biometric record (e.g., fingerprints);

4. Financial account information such as account numbers and balances, PINs, passwords, and security codes/questions required to access the account;

5. Taxpayer Identification Number;

6. Medical Information protected under the Health Insurance and Portability Accountability Act of 1996; and/or

7. Background investigations including reports or databases.

E. System/Record Owner is the FHFA employee responsible for planning, directing, and managing resources for an information system including electronic and paper-based files. The system/record owner functions as the information steward with the statutory or operational authority to establish the necessary controls for the generation, collection, processing, dissemination, security, and disposal of information.

F. System of Records, for purposes of the Privacy Act, means a group of records under the control of FHFA from which information is retrieved by the name of the individual or by some identifying number, symbol, or other particular assigned to the individual.

G. System of Records Notice is a public notice explaining a system of records maintained or controlled by the agency that may contain PII and the permitted uses of that information under the Privacy Act.

V. FUNCTIONAL RESPONSIBILITIES

A. Chief Privacy Officer is the agency's Senior Agency Official for Privacy and oversees the agency's collection, use, and protection of PII and is responsible for:

1. Establishing policy, procedures, and guidance for the use and protection of electronic and paper-based PII.

2. Monitoring FHFA's compliance with applicable privacy laws, regulations, guidelines, directives and reporting requirements.

3. Overseeing FHFA's privacy awareness training.

4. Developing and coordinating privacy notices, assessments, and documentation for FHFA systems.

5. Maintaining an inventory of FHFA systems that collect and maintain PII.

B. Chief Information Officer is responsible for:

1. Working with the CPO to oversee FHFA's cyber protection of PII.

2. Establishing IT policies, procedures, and controls to protect electronic files containing PII.

3. Providing data encryption tools and procedures.

4. Working with the CPO to ensure that FHFA complies with applicable privacy and information security laws, regulations, guidelines, directives and reporting requirements.

5. Establishing and implementing standard access control processes for FHFA systems.

C. Employees, contractor personnel, and entity personnel are responsible for:

1. Collecting, using, and protecting PII in accordance with applicable laws, regulations, policies, procedures, and SORNs.

2. Completing privacy awareness training.

D. Managers and supervisors are responsible for:

1. Ensuring that employees, contractor personnel, and entity personnel are aware of their responsibilities to adequately protect PII according to FHFA privacy policies and procedures.

E. Contracting Officer Technical Representatives are responsible for:

1. Instructing contractor personnel to protect adequately PII according to FHFA privacy policies and procedures.

F. Office of General Counsel is responsible for:

1. Providing legal advice and counsel on privacy-related issues, including review of policies, procedures, and other documents, as appropriate.

2. Approving *Federal Register* filings and rulemakings to include SORNs.

G. System/Record Owners are responsible for:

1. Reviewing, understanding, and securing the PII holdings maintained in their electronic or paper based files.

2. Overseeing the implementation of safeguards for the systems (electronic and paper-based files), for which they are responsible.

3. Authorizing user access to systems and records according to access control processes and periodically verifying user need and access to PII.

4. Instructing users on the proper use, security, and records retention requirements for the systems and records.

5. Completing privacy documentation (e.g., Privacy Impact Assessments) to document controls, identify privacy issues, and address actions needed to strengthen safeguards.

VI. AUTHORITY/REFERENCES

A. The Privacy Act of 1974, as amended, 5 U.S.C. 552a.

B. Section 208 and Title III, Federal Information Security Management Act of 2002, of the E-Government Act of 2002, Public Law 107-347.

C. Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H of the Consolidated Appropriations Act, 2005), Public Law 108-447.

D. Federal Housing Finance Agency Privacy Act Implementation, 12 C.F.R. part 1204.

ATTACHMENT A

Administrative Guide on Using and Protecting PII

I. COLLECTING, USING, SECURING, AND MAINTAINING PII

FHFA employees, contractor personnel, and entity personnel must protect PII that is under their control.

A. Securing Records, Files, and Work Areas

1. Store documents containing sensitive PII in a locked safe, locked file cabinet, or in a locked room.
2. If you have a laptop, secure your laptop with a cable lock.
3. When you leave your workstation or office, secure PII documents and your computer by:
    a. Placing documents containing sensitive PII in a locked drawer or cabinet, or locking your office door if it has a lock; and
    b. Locking your computer (using ctrl, alt, delete) and removing the access token.
4. Save electronic files in folders that have the access restricted to individuals who need the information to complete official business.
5. Do not save files containing sensitive PII (e.g., social security numbers, financial account information) to any non-FHFA device.
6. Follow FHFA's Information Security Policy Handbook and FHFA Information System Rules of Behavior, which contain requirements for FHFA information systems, such as system access, user IDs, passwords, encryption, remote media, and the use of FHFA computers, local drives and personal devices.
7. Ensure your FHFA Blackberry, laptop, and PII documents are secured when working remotely (e.g., telework from home, on-site at a regulated entity, or at a hotel or off-site conference).
8. Maintain official agency records according to FHFA's Records Management Policy and records management guidance.
9. Appropriately label all media and documents so that the user knows the sensitivity of the information and appropriately protects it.
10. Do not access FHFA documents and systems unless you are authorized to do so. If you are inadvertently given access to PII, report this to the CPO.
11. Do not disclose PII to people who are not authorized to receive the information or who do not have a legitimate business reason to have the information.

B. Copying, Printing, and Faxing

1. When making copies containing sensitive PII, remember to retrieve the originals and all copies from the copier.
2. Retrieve documents containing sensitive PII from shared printers as soon as they are printed. When available, print to printers located in secured rooms or to printers located in your office or workstation.
3. When faxing documents containing sensitive PII, promptly retrieve the original from the sending fax machine and alert the recipient to promptly retrieve the copy from the receiving fax machine.
4. When expecting a faxed document containing sensitive PII, monitor the fax machine closely and retrieve the fax as soon as it arrives. When available, use fax machines located in secured rooms.

C. Sending Packages and Documents within FHFA Facilities

1. Place documents in a sealed envelope that clearly identifies the recipient and is marked "to be opened by addressee only" or a similar notation. Do not place paper records containing sensitive PII in a "Holey Joe" type envelope.
2. Hand deliver packages containing sensitive PII to the addressee and confirm that the individual has received it.

D. Sending PII in E-mail

1. For email sent to another FHFA email account, do not send sensitive PII in the body of an FHFA email. Rather, send in an encrypted and password protected attachment.
2. Do not send PII, other than telephone number, physical address or e-mail address, in the body of any e-mail.
3. Do not send e-mail attachments containing sensitive PII to personal e-mail accounts, such as Yahoo, Gmail, or Hotmail.
4. Avoid sending e-mail attachments containing sensitive PII to non-FHFA e-mail address unless the attached file has been encrypted and password protected. Send the password in a separate communication.

E. Sending Packages by the US Postal Service or Commercial Carrier

1. Verify the recipient is authorized to receive the information as part of his/her official duties.
2. Send records in encrypted electronic files whenever possible.
3. Place paper documents in a sealed envelope that clearly identifies the recipient and is marked "to be opened by addressee only" or a similar notation.
4. Require an authorized signature upon delivery.

5. Track the shipment and follow-up with the recipient within 24 hours to ensure that the items sent have been received.
6. When sending documents/files containing sensitive PII, retain key tracking information in the event the package is lost, stolen, or compromised. If documents/files are lost, stolen, or compromised, the agency may need to identify the individuals affected and contact them with an action plan. Key tracking information is the information needed for the agency to respond to a breach, such as the source of the information, data fields containing PII, and formats in which the information is stored.

F. Carrying Records

1. Avoid carrying paper documents containing sensitive PII outside of an FHFA or a regulated entity facility. If you must carry documents containing sensitive PII outside of an FHFA or regulated entity facility, carry them in a secure package (e.g., sealed envelope) or briefcase.
2. Avoid carrying remote media such as CDs or thumb drives containing unencrypted sensitive PII outside of an FHFA or a regulated entity facility.
3. Secure and maintain control of briefcases, bags, and laptops when traveling. For example, if you leave your laptop in a vehicle, store it in the trunk or out of sight in the passenger compartment and lock the vehicle.

G. Disposing of Records

1. Follow FHFA's Records Management Policy and guidance on the disposal of agency records. Dispose of records containing PII by:
    a. Shredding paper documents, do not place them intact in a trash can or recycling bin;
    b. Deleting electronic files;
    c. Deleting electronic files containing PII within 90 days of when they are no longer needed; and
    d. Destroying and/or data wiping hard drives and remote media (e.g., CD, thumb drive).

H. Reporting Breaches Involving PII

1. Report any known or suspected breaches involving PII to the CPO within one hour of becoming aware of it. If the breach involved FHFA IT equipment, systems, or electronic data also contact the FHFA IT Help Desk.
2. When reporting to the CPO, provide as much information as possible, such as:
    a. Nature of the breach (e.g., lost files, stolen IT equipment, hacked computer access);

b. Information that was involved in the breach;

c. Date, time, and location;

d. Affected individuals; and

e. Any other pertinent information

3. For information on responding to known or suspected breaches involving PII, refer to the FHFA Breach Notification Policy and Plan.

II. SHARING PII

Before sharing PII outside of FHFA, employees and contractor personnel must contact the CPO to ensure that sharing the information complies with applicable privacy laws and FHFA privacy policies and SORNs. Prior to contacting the CPO, employees and contractor personnel must:

1. Identify what information will be shared, why the information will be shared, and with whom the information will be shared; and
2. Verify that FHFA has legal authority to share the information.

III. NEW DATA COLLECTION

Employees and contractor personnel must consult with the CPO when considering data collection involving PII from an individual, regulated entity, or other organization to determine what privacy requirements may apply. Examples of new data collections that may trigger privacy requirements include the following:

1. Developing or modifying an FHFA system;
2. Publishing a data collection form on the FHFA website;
3. Creating a data collection form;
4. Collecting new or modified data/information from a regulated entity;
5. Sending out an employee survey; and
6. Procuring a new system or service that will gather or store information about individuals.

Before collecting PII, System/Records Owners must:

1. Identify and document how the information will be used, controlled, and protected;
2. Verify that FHFA has legal authority to collect the information;
3. Verify that the data collection will be limited to what is relevant and is necessary to conduct official FHFA business;
4. Confirm that to the greatest extent possible, PII will be collected directly from the individual whom the information is about; and

5. Contact the CPO to determine if any of the following documentation is required.

Privacy Document	Applies To
Privacy Act Statement – A Privacy Act Statement is a notice provided to individuals when collecting PII. Privacy Act Statements inform the individual of the authority under which the information is collected; whether providing the information is voluntary or mandatory; the purpose for which the information will be used; routine uses of the information; and consequences, if any, to the individual for not providing the information.	Paper or electronic data collection forms that will be used to collect information from an individual.
Web Privacy Policy – For PII collected from the FHFA home page or web pages, a privacy policy or hyperlink to a privacy policy must be provided. The privacy policy must be machine-readable, automatically readable by a web visitor's browser, clearly labeled, easy to access, and written in plain language.	FHFA web pages
System of Records Notice (SORN) - A SORN is a public notice explaining a system of records maintained or controlled by the agency that may contain PII and the permitted uses of that information under the Privacy Act.	A group of any records under the control of FHFA from which information is retrieved by the name of the individual or by unique number, symbol, or other identifying particular assigned to the individual. Records can be paper or electronic.
Privacy Threshold Analysis (PTA) – A PTA is a screening tool used to identify privacy requirements for electronic systems.	Electronic systems

Privacy Document	Applies To
Privacy Impact Assessment (PIA) – A PIA is an analysis of how information is handled to (i) ensure handling conforms to applicable legal, regulatory, and policy requirements, (ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.	Electronic systems that contain PII

IV. CONSEQUENCES

Failure to comply with FHFA privacy policies and guidance may result in disciplinary action up to and including termination from the federal service. Violation of the Privacy Act may result in criminal and/or civil penalties.