FEDERAL HOUSING FINANCE AGENCY

Use and Protection of
Personally Identifiable Information Policy

Approved: SANDRA THOMPSON

Digitally signed by SANDRA THOMPSON
Date: 2024.12.05 15:07:21 -05'00'

Sandra L. Thompson, Director

Record of Revisions

Policy Version No.	Description	Date
1	• Final draft for review/approval	08/22/2010
2	• Updated Policy to include the Senior Agency Official for Privacy (SAOP) per OMB Memo No. M-16-24. • Updated the Authorities and References section of the policy to include the applicable statutes. • Updated the definition of a System of Records Notice (SORN) to match the definition in OMB Circular A-108. • Updated to make clear that employees and contractor personnel are required to report suspected and actual incidents/breaches to the Help Desk per FHFA's Information Security Incident and Breach Response Plan.	05/10/2022
3	• Updated the Procedures to add a Routine Use that is required by OMB for all non-exempt SORNs for data sharing in the event of a breach of PII or to assist another Federal Agency with its breach response. • Updated the Authorities and References to add OMB Memorandum M-17-12, FHFA Information Incident and Breach Response Plan, and FHFA Information System Rules of Behavior. • Updated the Appendix to add storage of PII to the description of how PII should be managed, to amend procedures for securing, protecting, and sending PII, and to include the current Privacy documents utilized in the Privacy Office.	07/25/2024

Use and Protection of
Personally Identifiable Information Policy

Table of Contents

I. POLICY

The Privacy Act of 1974 requires federal agencies to establish appropriate administrative, technical, and physical safeguards to protect agency records from threats which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. This document establishes the Federal Housing Finance Agency's (FHFA) policy on the collection, use, maintenance, storage, and security of personally identifiable information (PII).

II. DEFINITIONS

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

B. **Personally Identifiable Information (PII)** means 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, mother's maiden name, and truncated or partial social security numbers).

C. **Record** means any information maintained by the agency about an individual, 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 that is assigned to the individual, such as a fingerprint, 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. Some categories of PII are sensitive as standalone data, such as an individual's Social Security number, driver's license number, or other government-issued (including state-issued) identification number. Sensitive PII also includes an individual's name, home address, or telephone number in combination with any of the following:

1. Date or place of birth;

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

3. Financial account information, such as account numbers and balances, personal identification numbers (PINs), passwords, and security codes/questions required to access the account;

4. Taxpayer Identification Number (TIN);

5. Medical Information protected under the Health Insurance and Portability Accountability Act of 1996 (HIPAA);

6. Background investigations, including reports or databases; and/or

7. A full, truncated, or partial social security number.

E. **System/Record Owner** means 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** is a group of records under the control of FHFA from which information is retrieved by the name of the individual or by some other identifying number, symbol, or particular identifier assigned to the individual.

G. **System of Records Notice (SORN)** is a notice to the public published in the Federal Register about the existence and characteristics of a System of Records that must include: (i) the name and location of the system; (ii) the categories of individuals on whom records are maintained in the system; (iii) the categories of records maintained in the system; (iv) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (v) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (vi) the title and business address of the agency official who is responsible for the system of records; (vii) the agency procedures whereby an individual can be notified at their request if the system of records contains a record pertaining to them; (viii) the agency procedures whereby an individual can be notified at their request how they can gain access to any record pertaining to them contained in the system of records, and how they can contest its content; and (ix) the categories of sources of records in the system.

III. SCOPE

This policy applies to all FHFA employees, contractor personnel, and all other personnel whether or not from other entities (entity personnel) that have legal access to FHFA information systems (e.g., FHFA Office of Inspector General (OIG), Government Accountability Office (GAO), Office of Personnel Management (OPM), and other entities). The requirements of this policy pertain to all electronic systems and paper files that collect, use, maintain, store, and/or secure PII.

IV. PROCEDURES

The sections below outline specific requirements for protecting PII.

Collecting, Using, Sharing and Maintaining PII. PII must be collected, used, shared, and maintained in accordance with FHFA policy, guidance, procedures, and the applicable SORN. FHFA employees, contractor personnel, and entity personnel must:

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

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

C. Restrict access to only those individuals who need the PII to perform their official duties;

D. Immediately report all suspected or actual incidents and breaches to the FHFA Help Desk in accordance with the FHFA's Information Incident and Breach Response Plan;

E. Complete required annual privacy training and education and any required supplemental role-based privacy training; and

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

1. **Sharing PII.** Records containing PII may only be shared if authorized by law or with the express written consent of the individual whose PII is included in the record. Sharing any record containing PII is limited to the portion of the record necessary to complete the agency's business task.

Before sharing any information containing PII outside the agency, employees and contractor personnel must contact the Senior Agency Official for Privacy (SAOP) to ensure that the information containing PII complies with applicable privacy laws and FHFA privacy policies. This requirement does not apply to another federal agency for law enforcement purposes or to another federal agency in conducting personnel proceedings before any court or adjudicative or administrative body. This requirement does not apply to information necessary to respond to a breach either of the Agency's PII or, when appropriate, to assist another agency in its response to a breach. This requirement also does not apply 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.

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

3. **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.

V. RESPONSIBILITIES

A. 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; and

2. Approving Federal Register filings and rulemakings, including SORNs.

B. Senior Agency Official for Privacy (SAOP) is responsible for ensuring the agency's compliance with applicable privacy requirements, developing and evaluating privacy policies, and managing privacy risks consistent with the agency's mission through:

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; and

5. Maintaining an inventory of FHFA systems that collect and maintain electronic or paper-based PII.

C. **Chief Information Officer** is responsible for:

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

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

D. **Managers and supervisors** are responsible for:

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

E. **Employees, contractor personnel, and entity personnel** are responsible for:

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

2. Completing required privacy awareness training.

F. **Contracting Officer Technical Representatives** are responsible for:

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

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 (including 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 users continued need for access to PII;

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

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

VI. AUTHORITIES AND 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.

E. Executive Order No. 13719, Establishment of the Federal Privacy Council, 81 Fed. Reg. 7687 (Feb. 12, 2016).

F. OMB Memorandum No. M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 15, 2016).

G. OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.

H. OMB Memorandum No. M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017).

I. FHFA Information Incident and Breach Response Plan.

J. FHFA Information System Rules of Behavior (ROB).

VII. RECORDS RETENTION

This policy will be retained and managed in accordance with *FHFA Comprehensive Records Schedule (CRS)* Item 1.3b – Administrative Policies for 30 years. Agency records that result from the development and administration of this policy are retained and destroyed in accordance with the National Archives and Records Administration's General Records Schedule (GRS) Item 4.2.

APPENDIX

Administrative Guide on Using and Protecting PII

I. COLLECTING, USING, MAINTAINING, STORING, AND SECURING 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 (e.g., social security numbers, financial account information) in a locked safe, locked file cabinet, or in a locked room.
2. If you have a laptop, secure your laptop.
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 by removing the access token.
4. Save electronic files in folders that have the access restricted only 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-issued mobile device (e.g., cellphone or tablet), laptop, and all documents containing PII are secured when working remotely (e.g., telework, 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 (e.g., CUI-SP-PRVCY).
10. Do not access FHFA documents and systems unless you are authorized to do so. If you are inadvertently given access to PII, report the error to the Help Desk.
11. Do not disclose PII to anyone not authorized to receive the information or

who does 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, use the fax function of the email system, or if using a fax machine, be sure to retrieve the original copy from the 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 possible, use the fax function of the FHFA email system.

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 into an envelope that is transparent or otherwise not opaque.
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, and provide the password in a separate email or by another mode of communication.
2. Do not send any 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. The only exception is that staff is permitted to send their own eOPF forms to their personal e-mail accounts.
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 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 business carrying case.
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

Follow FHFA's Records Management Policy and guidance on the disposal of agency records. Dispose of records containing PII by:

1. Shredding paper documents; do not place them intact in a trash can or recycling bin;
2. Deleting electronic files;
3. Deleting electronic files containing PII within 90 days of when they are no longer needed; and
4. Destroying and/or data wiping hard drives and remote media (e.g., thumb drive).

H. Reporting Incidents and Breaches Involving PII

1. Immediately report all suspected or actual information incidents and breaches to the FHFA Help Desk in accordance with FHFA's Information Incident and Breach Response Plan.
2. When reporting any suspected or actual information incident or breach to the Help Desk, the reporting employee, contractor personnel, or entity personnel must provide as much information as possible, such as: the nature of the incident or breach (e.g., lost files, stolen IT equipment, hacked computer access); the information that was involved in the incident or breach; the date, time, and location; the number of affected individuals; and any other pertinent information.

II. SHARING PII

Before sharing PII outside of FHFA, employees, contractor personnel, and all other personnel must ensure that sharing the PII complies with applicable privacy laws, FHFA's privacy policies, and the applicable SORN(s). Employees and contractor personnel should contact the Privacy Office if unsure about whether they have authority to share the information containing PII.

III. NEW DATA COLLECTION

Employees and contractor personnel must consult with the Privacy Office when considering new data collections involving PII. Examples of new data collections that may trigger privacy requirements include the following:

- **A.** Developing or modifying how PII is managed or used in a FHFA system;
- **B.** Publishing a data collection form on the FHFA website;
- **C.** Creating a data collection form;
- **D.** Collecting new or modified data from a regulated entity;
- **E.** Sending out an employee survey; and
- **F.** Procuring a new system or service that will gather or store PII.

Before collecting PII, System/Records Owners must:

- **A.** Identify and document how the information will be used, controlled, and protected;
- **B.** Verify that FHFA has legal authority to collect the information;
- **C.** Verify that the data collection will be limited to what is relevant and is necessary to conduct official FHFA business;
- **D.** Confirm that to the greatest extent possible, PII will be collected directly from the individual described by the information; and
- **E.** Contact the SAOP to determine if any of the following documentation is required:

Privacy Document	Applies To
Privacy Act Statement (PAS) – A PAS is a statement or notice required by the Privacy Act that notifies the public of the authority, purpose, and routine uses for collecting personal information. The PAS also notifies the public or users on whether providing such information is voluntary or mandatory and the effects, if any, of not providing all or any portion of the requested information.	Paper or electronic data collection forms that will be used to collect information from an individual.

Privacy Document	Applies To
Website Privacy Policy – The Website Privacy Policy provides information to the public about how PII collected on one of FHFA's public-facing websites will be used. The agency's privacy policy or hyperlink to the privacy policy must be provided for PII collected from any webpages on FHFA's websites. 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 notice to the public published in the Federal Register about the existence and characteristics of a system of records that must include: (i) the name and location of the system; (ii) the categories of individuals on whom records are maintained in the system; (iii) the categories of records maintained in the system; (iv) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (v) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (vi) the title and business address of the agency official who is responsible for the system of records; (vii) the agency procedures whereby an individual can be notified at their request if the system of records contains a record pertaining to them; (viii) the agency procedures whereby an individual can be notified at their request how they can gain access to any record pertaining to them contained in the system of records, and how they can contest its content; and (ix) the categories of sources of records in the system.	A group of any records under the control of FHFA from which information is retrieved by PII. Records can be paper or electronic.

Privacy Document	Applies To
Privacy Security Questionnaire (PSQ) – A PSQ is a document used to determine whether a program or system has privacy implications and if additional privacy compliance documentation is required, such as a Privacy Impact Assessment or SORN. This questionnaire replaces the Privacy Threshold Analysis (PTA).	Electronic systems.
Privacy Impact Assessment (PIA) – A PIA is an analysis of how information is used (i) to ensure use conforms to applicable legal, regulatory, and policy requirements, (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (iii) to 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.