U.S. Department of Housing and Urban Development (HUD) Privacy Policy

April 15, 2020

I. Introduction

The U.S. Department of Housing and Urban Development’s (HUD) Privacy Program mission is to protect and minimize impacts on the privacy of individuals, while achieving HUD’s mission. HUD’s Privacy Program is administered by the Privacy Office within HUD’s Office of Administration and is led by HUD’s Senior Agency Official for Privacy (SAOP) and its Chief Privacy Officer (CPO). The Privacy Office implements requirements of the Privacy Act of 1974, as amended; E-Government Act of 2002; and the Federal Information Security Modernization Act (FISMA), as well as policy directives and best practices issued in furtherance of those Acts.

This policy establishes a set of privacy principles and applies those principles to employees, individuals applying for HUD programs, business partners, contractors and clients. These principles and policy requirements govern how HUD processes Personally Identifiable Information (PII, see definition further below) and explains how HUD complies with the privacy requirements. It is imperative that all HUD personnel physically involved in the processing of PII understand and comply with the requirements set forth in this policy.

PII refers to information which can be used to distinguish or trace a data subject’s identity, either alone or when combined with other information that is linked or linkable to a specific individual, such as information relating to FHA loan participants or individual HUD employees or contractors. Set forth below is a non-exclusive list of information that may constitute PII on its own or in combination with other information:

- Full name
- Home address
- Business Contact Information (see definition)
- Personal e-mail address
- Social security number
- Passport number
- Driver’s license number
- Certificate number
- Credit card numbers
- Date of birth
- Telephone number
- Log in details
- Personnel number
- Vehicle identifier or serial number
- Photograph or video identifiable to an individual
- Biometric information
- Medical information
- Criminal history
- Other information related to an individual that may directly or indirectly identify that individual (e.g., salary, performance rating, purchase history, call history, etc.)
HUD personnel must consider the sensitivity of the PII based on the complete context in which it appears and/or processed. Each element of PII may be considered sensitive under certain circumstances, such as in association with a list of individuals under investigation. Questions or inquiries about HUD’s Privacy Program should be sent to the Privacy Office.

II. Exclusions

This policy is affiliated with HUD’s collection and handling of personal information. HUD follows certain exceptions outlined in the Privacy Act of 1974. Examples of exceptions include records containing classified information on national security and those concerning criminal investigations. Additionally, certain exceptions may be defined in procedure when only business contact information is processed, such as when business e-mails are exchanged or when business contact information is used to print badges for a meeting. Other exceptions to this policy are expected to be requested only in unusual or exceptional circumstances and should be documented and approved by HUD's SAOP.

III. Privacy Requirements

The following principles apply to the processing of PII. These principles are based on the Fair Information Practice Principles (FIPPs) and are mirrored in several national and international privacy laws and regulations, as well as in the laws of many U.S. states.

A. Access and Amendment

HUD should provide individuals with appropriate access to PII and the opportunity to correct or amend PII. HUD should establish procedures to allow data subjects reasonable and appropriate access to PII and should respond to access requests within a reasonable timeframe.

B. Transparency

HUD should be transparent and notify individuals regarding the creation, collection, use, processing, storage, dissemination, maintenance, and disclosure of PII.

C. Individual Participation

HUD should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. HUD should also provide mechanisms for appropriate access, correction, and redress regarding use of PII. Individuals may address concerns or complaints to HUD’s SAOP.

D. Purpose Specification and Use Limitation:

HUD should specify the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used. HUD should use, process, store, maintain, disseminate, and disclose PII solely for the purpose(s) specified in the notice, and sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
E. Data Minimization:

HUD should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

HUD’s Privacy Office maintains an inventory of PII holdings and uses the PTA, PIA, and SORN processes to identify methods to further reduce the data the Agency collects and to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete.

F. Data Quality and Integrity:

HUD should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete to ensure fairness to the individual.

G. Security:

HUD should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. Detailed guidance for PII Handling is provided in Section IV of this policy.

H. Federal Reporting Mandates

HUD should abide by all federal reporting mandates and deadlines. HUD should maintain an archive of all documents submitted per federal reporting mandates. Information that needs to be included in reports should be regularly maintained in a manner that facilitates efficient access and consolidation for compiling reports.

I. Accountability and Auditing:

HUD should be accountable for complying with these requirements, providing training to personnel who use or process PII, and auditing the actual use of PII to demonstrate compliance with applicable privacy protection requirements. Additionally, HUD should incorporate key privacy requirements into the Agency’s Rules of Behavior. Violations of rules and requirements will be recorded by the Privacy Liaison Officer of each office.
J. Federal Record Rights

In accordance with federal regulation, HUD should provide notice describing the individual data subject’s rights in relation to personal data as follows:

- The individual data subject has access to the personal data held by HUD about them.
- The individual data subject can correct a record that is inaccurate, irrelevant, or incomplete.

Additionally, HUD should provide public access to information and instructions regarding the process and contacts for making a request to correct any record pertaining to the individual.

K. System of Records Notice

A System of Records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. HUD adheres to the Privacy Act requirements for publishing publish notices of its systems of records in the Federal Register, which are referred to as SORNs.

Each System of Records Notice (SORN) describes what, why and how HUD collects, maintains, uses and disseminates records in the system. Some systems maintain information on HUD employees while others maintain information from or about individuals outside of HUD. These Government-wide systems are maintained by other Federal agencies that hold some of the operating authority over the records such as the Office of Personnel Management's Employee Performance File system.

L. Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form is collected, maintain, stored, and disseminated, in addition to examining and evaluating the privacy risks and the protections and processes for handling information to mitigate those privacy risks. A PIA is required when HUD develops, procures, or uses information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

M. Definitions

Business Contact Information – Information that is limited to an individual's name and one or more of the following: organization name, organizational title, organizational role, business address, business telephone number (including business cell phone number) and business e-mail address.
Data Subject – A natural person who can be identified, directly or indirectly, by reference to an identification number or factors specific to his or her physical, physiological, mental, economic, cultural or social identity. A data subject is an end user whose personal data can be collected.

Personally Identifiable Information (PII) – Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Personnel – Current, former and prospective employees and contractors of HUD. The Personnel relationship is triggered by documentation that establishes the personnel relationship between HUD and the individual (e.g., job application, offer letter, agreement or other similar documents).

Process or Processing – Any operation or set of operations that is performed in regards to PII, whether or not by automated means, such as collection, recording, organization, storage, adaptation, or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

Privacy Act of 1974 (5 U.S.C. § 552a) – A code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

IV. Personally Identifiable Information (PII) Handling

HUD requires strict handling guidelines for employees and contractors who handle PII due to the nature of the data and the increased risk to an individual if data were to be compromised.

A. General Handling

Methods for handling PII include, but are not limited to the following, and must be done in accordance with HUD’s approved records schedules:

- Store sensitive PII on secure HUD network, systems, and HUD-approved media;
- Secure sensitive paper PII data by locking it in desks and filing cabinets;
- Remove visible PII from desks and office spaces when not in use (e.g., at the end of each day);
- Destroy sensitive PII by shredding;
- Delete sensitive electronic PII by emptying computer “recycle bin”;
- Only use HUD-provided email addresses for conducting official business; and
- Encrypt sensitive PII on computers, media, and other devices, especially when sending data outside of HUD’s network.
B. Distribution and Transmission

Sensitive PII may be distributed or released to other individuals only if: (1) it is within the scope of the recipient's official duties; (2) the recipient has an official, job-based need to know; (3) the distribution is done in accordance with a legitimate underlying authority (e.g., a routine use to a SORN); and (4) sharing information is done in a secure manner. When in doubt HUD employees must treat PII as sensitive and must keep the transmission of sensitive PII to a minimum, even when it is protected by secure means.

Other ways for communicating, sending, and receiving sensitive PII include:

- **Facsimile** – When faxing information, HUD personnel should include an advisory statement about the contents on the cover sheet and should notify the recipient before and after transmission.
- **Mail** – HUD personnel should physically secure PII when in transit by sealing it in an opaque envelope or container, and mail it using First Class or Priority Mail, or a comparable commercial service. HUD personnel should not mail, or send by courier sensitive PII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted.
- **Email** – When emailing Sensitive PII outside of HUD, save it in a separate document and password-protect or encrypt it. Send the encrypted document as an email attachment and provide the password to the recipient in a separate email or by phone.
  - Never email sensitive PII to personal email accounts or devices.
- **Hard Copy** – HUD personnel should also hand-deliver documents containing sensitive PII whenever needed. HUD personnel should not leave sensitive PII unattended on printers, facsimile machines, copiers, or in other common places.

**Dates and Notices**

**Date of Last Review:** April 2020

**Date of Last Revision:** April 2020