U.S. Department of Housing and Urban Development
Office of Public and Indian Housing

SPECIAL ATTENTION OF:
Directors of HUD Regional and Field Offices of Public Housing;
Public Housing Agencies that Receive Funds under Any Public and Indian Housing Program

NOTICE PIH-2015-06

Issued: April 23, 2015

Expires: Effective until amended, superseded, or rescinded

Cross References:
PIH 2014-10, PIH 2010-15

Subject: U.S. Department of Housing and Urban Development (HUD) Privacy Protection Guidance for Third Parties

1) **Purpose**: This notice informs all public housing agencies (PHAs) about their responsibilities for safeguarding personally identifiable information (PII) required by HUD and preventing potential breaches of this sensitive data. HUD is committed to protecting the privacy of individuals' information stored electronically or in paper form, in accordance with federal privacy laws, guidance, and best practices. HUD expects its third party business partners, including Public Housing Authorities, who collect, use, maintain, or disseminate HUD information to protect the privacy of that information in accordance with applicable law.

   PIH 2014-14 is being revised to include guidance to assist PHA system administrators and users to fulfill their requirements for information technology security awareness training.

2) **Background**: Section 6 of the Housing Act of 1937, the Privacy Act of 1974, 5 U.S.C. § 552a (Privacy Act), The Freedom of Information Act (FOIA), 5 U.S.C. § 552, and Section 208 of The E-Government Act are the primary federal statutes that limit the disclosure of information about public housing residents and recipients of the Housing Choice Voucher program. In addition, the Housing and Community Development Act of 1987, 42 U.S.C. § 1437d (q)(4), 42 U.S.C. § 1437d (t)(2), 42 U.S.C. § 3543, and the Stewart B. McKinney Homeless Assistance Act of 1988, 42 U.S.C. § 3544, further regulate the treatment of this information.

   a) General HUD program requirements are set forth in 24 C.F.R. Part 5, Subpart B, Disclosure and Verification of Social Security Numbers and Employer Identification Numbers: Procedures for Obtaining Income Information. Subpart B enables HUD and

PHAs to obtain income information about applicants and participants in the covered programs through computer matches with State Wage Information Collection Agencies (SWICAs) and Federal agencies, in order to verify an applicant's or participant's eligibility for or level of assistance.

i) *Restrictions on Use of Income Information Obtained from SWICA and Federal Agencies.* The restrictions of 42 U.S.C. 3544(c)(2)(A) apply to the use by HUD or a PHA of income information obtained from a SWICA and the restrictions of 42 U.S.C. 3544(c)(2)(A) and of 26 U.S.C. 6103(l)(7)(C) apply to the use by HUD or a PHA of income information obtained from the Internal Revenue Service or the Social Security Administration.

b) The Privacy Act and other requirements for grants and contracts is spelled out in 24 C.F.R. 5.212 which states:

i) *Compliance with the Privacy Act*. The collection, maintenance, use, and dissemination of SSNs, EINs, any information derived from SSNs and Employer Identification Numbers (EINs), and income information under this subpart shall be conducted, to the extent applicable, in compliance with the Privacy Act (5 U.S.C. 552a) and all other provisions of Federal, State, and local law.

Privacy Act Notice. All assistance applicants shall be provided with a Privacy Act notice at the time of application. All participants shall be provided with a Privacy Act notice at each annual income recertification.

c) The Federal Acquisition Regulation (FAR), 48 C.F.R. 24.104, sets forth that compliance with the requirements of the Privacy Act be included in HUD contracts at clause 52.224-2, which provides in part:

(a) The Contractor agrees to—
(1) *Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act ….*

Similar language is included in all HUD Grant Agreements requiring the Grantee to comply with the provisions of the Privacy Act of 1974 and the agency rules and regulations issued under the Act. (See Attachments 1 and 2 for the above provisions)

d) Additional federal guidance on privacy protection is in OMB privacy-related memoranda, including:

i) OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy

ii) OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

iii) OMB M-04-26, Personal Use Policies and ―File Sharing Technology

iv) OMB M-05-08, Designation of Senior Agency Officials for Privacy

v) OMB M-06-15, Safeguarding Personally Identifiable Information

vi) OMB M-06-16, Protection of Sensitive Agency Information

vii) OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments

viii) OMB Memo, September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification Guidance

ix) OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

x) OMB M-14-04, FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (FISMA). FISMA requires federal agencies to implement a mandatory set of processes designed to ensure the confidentiality, integrity, and availability of system related information. FISMA requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely, and efficient manner.

e) Definitions

As used in this Notice, the following terms are defined as:

i) Personally Identifiable Information (PII). Defined in OMB M-07-16 as ". . . information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

ii) Sensitive Personally Identifiable Information. PII that when lost, compromised or disclosed without authorization could substantially harm an individual. Examples of sensitive PII include social security or driver's license numbers, medical records, and financial account numbers such as credit or debit card numbers.

3) **Guidance on Protecting Sensitive Privacy Information**: The Privacy Act requires that federal agencies maintain only such information about individuals that is relevant and necessary to accomplish its purpose. The Privacy Act also requires that the information be maintained in systems or records – electronic and paper – that have the appropriate

administrative, technical, and physical safeguards to protect the information, however current. This responsibility extends to contractors and third party business partners, such as Public Housing Authorities, who are required to maintain such systems of records by HUD.

a) Contractors and third party business partners should take the following steps to help ensure compliance with federal requirements:

i) Security Awareness and Privacy Training

(1) The National Institute of Standards and Technology (NIST) publishes templates and guides for what security awareness trainings should entail in order to be FISMA compliant. These guidelines focus on the following key aspects:

- **Confidentiality** - Protecting information from unauthorized access and disclosure.
- **Integrity** - Assuring the reliability and accuracy of information and IT resources by guarding against unauthorized information modification or destruction.
- **Availability** - Defending information systems and resources to ensure timely and reliable access and use of information. As such, systems are vulnerable to misuse, interruptions and manipulation.
- **Threat**- A threat in the case of IT security is the potential to cause unauthorized disclosure, unavailability, changes, or destruction of protected information.
- **Vulnerability**- Any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy
- **Risk** is the likelihood that a threat will exploit vulnerability.
- **Controls** are policies, procedures, and practices designed to decrease the likelihood, manage the impact, or minimize the effect of a threat exploiting a vulnerability

(2) Additionally, the NIST provides publications for reference on Building an Information Technology Security Awareness and Training Program and Security and Privacy Controls for Federal Information Systems and Organizations

(3) PHAs should maintain adequate documentation that supports the training for all staff as well as maintain auditable records of training completion. Although there is not required reporting on the training, Office of Field Operations personnel may spot-check compliance on on-site visits.

ii) Limit Collection of PII

(1) Do not collect or maintain sensitive PII without proper authorization. Collect only the PII that is needed for the purposes for which it is collected.

(2) Consistent with the provisions of this Notice, PHAs may enter into agreements (or in some cases be required) to provide PII to legitimate researchers under contract

or other agreement with HUD to support studies on the effects and operations of HUD programs. Further, HUD encourages PHAs to supply PII to other legitimate researchers who do not have contracts or other agreements with HUD in support of such studies, so long as the PHA in question has taken reasonable precautions to prevent disclosure of PII outside of the research team. Such reasonable precautions generally involve written agreements between the PHA and one or more researchers that specify the legal obligations of the latter to protect PII from disclosure.

iii) Manage Access to Sensitive PII

(1) Only share or discuss sensitive PII with those personnel who have a need to know for purposes of their work. Challenge anyone who asks for access to sensitive PII for which you are responsible.

(2) Do not distribute or release sensitive PII to other employees, contractors, or other third parties unless you are first convinced that the release is authorized, proper and necessary.

(3) When discussing sensitive PII on the telephone, confirm that you are speaking to the right person before discussing the information and inform him/her that the discussion will include sensitive PII.

(4) Never leave messages containing sensitive PII on voicemail.

(5) Avoid discussing sensitive PII if there are unauthorized personnel, contractors, or guests in the adjacent cubicles, rooms, or hallways who may overhear your conversations.

(6) Hold meetings in a secure space (i.e., no unauthorized access or eavesdropping possible) if sensitive PII will be discussed and ensure that the room is secured after the meeting.

(7) Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII.

(8) Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.

iv) Protect Hard Copy and Electronic Files Containing Sensitive PII

(1) Clearly label all files containing sensitive PII by placing appropriate physical labels on all documents, removable media such as thumb drives, information systems, and application. Examples of appropriate labels might include ―For Official Use Only or ―For (Name of Individual/Program Office) Use Only.

(2) Lock up all hard copy files containing sensitive PII in secured file cabinets and do not leave unattended.

(3) Protect all media (e.g., thumb drives, CDs, etc.,) that contain sensitive PII and do not leave unattended. This information should be maintained either in secured file cabinets or in computers that have been secured.

(4) Keep accurate records of where PII is stored, used, and maintained.

(5) Periodically audit all sensitive PII holdings to make sure that all such information can be readily located.

(6) Secure digital copies of files containing sensitive PII. Protections include encryption, implementing enhanced authentication mechanisms such as two-factor authentication, and limiting the number of people allowed access to the files.

(7) Store sensitive PII only on workstations that can be secured, such as workstations located in areas that have restricted physical access.

v) Protecting Electronic Transmissions of Sensitive PII via fax, email, etc.

(1) When faxing sensitive PII, use the date stamp function, confirm the fax number, verify that the intended recipient is available, and confirm that he/she has received the fax. Ensure that none of the transmission is stored in memory on the fax machine, that the fax is in a controlled area, and that all paper waste is disposed of properly (e.g., shredded). When possible, use a fax machine that uses a secure transmission line.

(2) Before faxing PII, coordinate with the recipient so that the PII will not be left unattended on the receiving end.

(3) When faxing sensitive PII, use only individually-controlled fax machines, not central receiving centers.

(4) Do not transmit sensitive PII via an unsecured information system (e.g., electronic mail, Internet, or electronic bulletin board) without first encrypting the information.

(5) When sending sensitive PII via email, make sure both the message and any attachments are encrypted.

(6) Do not place PII on shared drives, multi-access calendars, the Intranet, or the Internet.

vi) Protecting Hard Copy Transmissions of Files Containing Sensitive PII

(1) Do not remove records about individuals with sensitive PII from facilities where HUD information is authorized to be stored and used unless approval is first obtained from a supervisor. Sufficient justification, as well as evidence of information security, must been presented.

(2) Do not use interoffice or translucent envelopes to mail sensitive PII. Use sealable opaque solid envelopes. Mark the envelope to the person's attention.

(3) When using the U.S. postal service to deliver information with sensitive PII, double-wrap the documents (e.g., use two envelopes – one inside the other) and mark only the inside envelope as confidential with the statement ―To Be Opened By Addressee Only.

vii) Records Management, Retention, and Disposition

(1) Follow records management laws, regulations, and policies applicable within your jurisdiction.

(2) Ensure all Public Housing Authority locations and all entities acting on behalf of the Authority are managing records in accordance with applicable laws, regulations, and policies.

(3) Include records management practices as part of any scheduled oversight protocols.

(4) Do not maintain records longer than required.

(5) Destroy records after retention requirements are met.

(6) Dispose of sensitive PII appropriately – use cross-cut shredders or burn bags for hard copy records and permanently erase (not just delete) electronic records.

viii) Incident Response

(1) Supervisors should ensure that all personnel are familiar with reporting procedures.

(2) Promptly report all suspected compromises of sensitive PII related to HUD programs and projects to HUD's National Help Desk at 1-888-297-8689.

ix) Contact Information

Inquiries about this notice should be directed to Matthew Steen, Privacy Liaison Officer, Real Estate Assessment Center, Office of Public and Indian Housing, at 202-475-8933.

x) **Paperwork Reduction Act**. The information collection described in this Notice has been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C 3520). In accordance with the PRA, HUD may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the collection displays a currently valid OMB control number.

/s/

Lourdes Castro Ramírez,
Principal Deputy Assistant Secretary for
Public and Indian Housing