Chapter 17

CRIMINAL RECORDS and RECORDS MANAGEMENT POLICY

INTRODUCTION

In the course of its regular operations, IHA comes into possession of criminal records, as well as other documents related to criminal offenses of applicants (i.e. drug and alcohol abuse treatment documentation). While necessary to accomplish Housing Authority business, these records must be maintained securely and kept from improper use.

The Housing Authority may also be called upon to perform criminal record and other record checks regarding applicants or tenants for housing that receives federal assistance from IHA. IHA shall maintain the records received for these residents or applicants in the manner prescribed in this policy.

A. ACQUISITION

All adult applicants shall complete the IHA Information Release Form authorizing the release of criminal record history to the Authority upon applying for housing, or at any time an existing resident household wishes to add an adult member to the lease. Criminal background check will be performed by an approved third-part service of the IHA Administration's choice. This check is done for the purpose of screening adult applicants for housing.

All requests for criminal records and records relating to criminal history shall be sent to the program staff. Only the designated program staff, appropriate personnel, and the Hearing Officer, shall have access to these records. The program staff, appropriate personnel, and Hearing Officer shall discuss the records with other Authority employees only as required to make a housing decision.

B. MAINTENANCE

The Authority will keep all criminal records or records relating to criminal history that are received confidential. These records will be used only to screen applicants for housing or to pursue evictions. The records will not be disclosed to any person or entity except for official use in the application process, hearing process, in accordance with the regulations, and/or in court proceedings. No copies will be made of the records except as required for official or court proceedings.

Criminal records or records relating to criminal history status are maintained in the applicant or resident file in a secured area, or will be maintained in a separate file in a secured area. These

files are maintained in locked cabinetry in a secured office with limited access. The program staff and appropriate personnel are the only employees having access to the cabinet or to the office.

C. DISPOSITION

The records shall be disposed of within the policies of the IHA. If contested, the police records shall be retained until all issues are resolved. In the event eligibility is denied, the records will be destroyed 3 years after determination of ineligibility or at the conclusion of 60 calendar days for a determination of eligibility, whichever is applicable for the case, after such time is afforded the applicant or resident the opportunity a hearing. The 60 calendar days may be extended in order to complete an action underway (i.e. Hearing, court proceeding, fair housing requirements, etc.), but the record will be destroyed upon finalization of action. In the event that the applicant is approved and moved into a PH unit, then that criminal background record will be shredded and listed on the Criminal Background Shred Record that we have maintained on our Server.

D. PRIVACY PROTECTION on RECORDS (PIH 2010-15 and update PIH 2014-10)

Overview

IHA is responsible for safeguarding personally identifiable information (PII) required by HUD and preventing potential breaches of this sensitive data. IHA and 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 IHA and other parties who collect, use, maintain, or disseminate HUD information to protect the privacy of that information in accordance with applicable law.

General HUD program requirements are set forth in 24 C.F.R. Part 5. Compliance with 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.

ii) *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. The Federal Acquisition Regulation (FAR), 48 C.F. R. Subpart 1524.1, sets forth that compliance with the requirements of the Privacy Act be included in HUD contracts at clause 52.224-2.

Personally Identifiable Information (PII)

The PII is 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."

Sensitive Personally Identifiable Information

Sensitive Personally Identifiable Information is defined as 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.

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 IHA, who are required to maintain such systems of records by HUD.

IHA will take the following steps to help ensure compliance with these requirements:

i) 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.

ii) 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.

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

(5) 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.

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

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

iii) 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.

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

(5) 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.

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

iv) 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.

v) 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”

vi) Records Management, Retention and Disposition

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

(2) Ensure all IHA 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.

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

vii) 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 the Executive Director.