Office of Native American Programs
Office of Public & Indian Housing

**No. 2014-05(R)**
**June 05, 2014**

# PROGRAM GUIDANCE

**PROGRAM:** All Grant Programs

**FOR:** Tribal Government Leaders, Tribally Designated Housing Entities, and the Department of Hawaiian Home Lands

**FROM:** For Rodger J. Boyd, Deputy Assistant Secretary for Native American Programs, PN

**TOPIC:** Protecting Personal Information

**PURPOSE:** The purpose of this guidance is to provide procedures for protecting personal information when sharing data with HUD's Office of Native American Programs (ONAP).

**BACKGROUND:** If an individual can be identified through personal information in a document or collection of documents, privacy protection actions should be implemented. Federal employees are responsible for respecting and protecting personally identifiable information. The Privacy Act of 1974 (5 USC § 552a) and the E-Government Act of 2002 (44 USC § 101) govern how Federal agencies gather use, maintain, and disseminate personal information.

This guidance complements Notice PIH 2014-10, which describes HUD's procedures for protecting sensitive personal information. The Notice is available at: http://portal.hud.gov/hudportal/HUD?src=/program_offices/public_indian_housing/publications/notices.

There are instances when ONAP requires information from recipients of HUD grants to assess and verify compliance with pertinent statutes and regulations. Some of this information may contain personal data such as full names, Social Security numbers, street addresses, internet addresses, telephone numbers, photographs, vehicle registration ID numbers, driver's license numbers, and the like. Documentation that may contain personally identifiable information include payroll journals, checks, check registers, contracts or contract registers, invoices, tenant files, etc.

Not all personal information is considered sensitive because many people share the same trait. This includes information such as first or last name (if common), country, state, or city of residence, age (especially if non-specific), gender or race, names of schools attended, and work place, pay grade, salary, or job position.

Recipients and ONAP staff should follow the procedures described below to protect personally identifiable information in documentation submitted to ONAP.

**Recipient Responsibilities.** Protecting personally identifiable information starts with the recipient. Prior to sending documents to ONAP, it is strongly recommended that the recipient carefully review the documentation that ONAP requests to determine if it contains personal information. If the documentation does contain personal information, the recipient should determine whether ONAP needs the personal information. ONAP is available to assist a recipient in making this determination.

If ONAP does not need to see the personal information the recipient must redact or hide all information that could identify a person. This can be done with a black marker or correction fluid.

When ONAP requires personal information to address a specific performance or compliance issue (for example, the recipient may be requested to submit tenant information so that ONAP can verify participant eligibility) the personal information cannot be redacted. Documents containing personal information must be sent to ONAP in a manner that protects the personal information.

When sending personal information to ONAP by the U.S. Postal Service, place the documentation in two envelopes and state the following on the inner envelope: To Be Opened by Addressee Only.

If the recipient sends the documentation as an email attachment, the recipient can encrypt the file containing the scanned documents and send them to ONAP as an email attachment.

To encrypt a file in Windows, follow the steps described below.

1. Right-click the folder or file you want to encrypt, and then click **Properties**.
2. Click the **General** tab, and then click **Advanced**.
3. Select the **Encrypt contents to secure data** check box, click **OK**, and then click **OK** again.

NOTE: The first time you encrypt a folder or file, an encryption certificate is automatically created. You should back up your encryption certificate. If your certificate and key are lost or damaged, and you don't have a backup, you won't be able to use the files that you have encrypted. For more information, see http://windows.microsoft.com/en-us/windows/back-up-efs-certificate#1TC=windows-7.

**ONAP Staff Responsibilities.** Staff should make certain to respect and protect the privacy of an individual's personal information. Specific actions to be taken include the following.

If personal information is required to verify compliance, request that the recipient encrypt the document and send it as an email attachment. The recipient may also send the information by fax or regular mail, as long as unneeded personal information is redacted or blackened out prior to sending the information to HUD.

If the recipient submits documentation that contains unneeded personal information, HUD staff should contact the grantee and request redacted versions. Immediate steps should be taken to destroy documents that have not been redacted.

To de-encrypt a folder or file, follow the steps described below.

1. Right-click the folder or file you want to decrypt, and then click **Properties**.
2. Click the **General** tab, and then click **Advanced**.
3. Clear the **Encrypt contents to secure data** check box, click **OK**, and then click **OK** again.

Previously submitted documentation that contains personally identifiable information should be maintained according to HUD's document security protocols.

**ADDITIONAL GUIDANCE:** Contact your Area ONAP if you have any questions.