Finding HCV11

HCVP PII Memo

In this finding, please find the following:

a. HCVP PII Memo
    i. Memo regarding personally identifiable information (PII) that all staff must agree to

District of Columbia Housing Authority
1133 North Capitol Street N.E.,
Washington, DC 20002-7599
(202) 535-1000 | dchousing.org

Brenda Donald, Executive Director

HOUSING CHOICE VOUCHER PROGRAM

Memorandum

To: **All Housing Choice Voucher Program Staff**

From: **Quality Assurance Division**

Date:

Re: **Personally Identifiable Information (PII) and Information Sharing**

HCVP is committed to protecting the privacy of individuals' information stored electronically or in paper form in accordance with the Privacy Act of 1974 and other federal privacy-related laws, guidance and best practices. In an effort to avoid potential data breaches, it is imperative for staff to protect Personally Identifiable Information (PII) at all levels of communication.

What is PII?

PII is any information that can uniquely identify people as individuals separate from all others. It may include the following:

- Name
- address
- email
- telephone number
- date of birth
- passport number
- fingerprint
- driver's license number
- credit or debit card number
- Social Security number
- tax information

Sensitive PII is PII that when lost, compromised, or disclosed could substantially harm an individual. Examples of sensitive PII include social security or driver's license numbers, medical records and financial account numbers.

Why does PII need to be secured?

Protecting PII is essential for personal privacy, data privacy, data protection, information privacy and information security. With just a few bits of an individual's personal information, thieves can create false

accounts in the person's name, incur debt, create a falsified passport or sell a person's identity to a criminal. Sensitive PII is information that, when disclosed, could result in harm to the individual if a data breach occurs. A **data breach** occurs when PII is viewed, leaked, or accessed by anyone who is not the individual or someone authorized to have access to the information as part of his/her official duties.

Steps to take to ensure compliance

HCVP staff should take the following steps to help ensure compliance with the Privacy Act and other privacy-related laws:

1. Do not collect or maintain sensitive PII without proper authorization; collect only the PII that is needed for HCVP purposes

2. Do not distribute or release sensitive PII to others until the release is authorized.

3. Before discussing sensitive PII over the telephone, confirm that you are speaking to the correct person and inform him/her that the discussion will include sensitive PII. Do not leave messages containing sensitive PII on voicemail.

4. Shred important documents before discarding them. Do not remove records with sensitive PII from any DCHA offices.

5. Do not send sensitive PII via emails unless authorization to do so is given. For any request for information outside of the scope of assigned work is requested, the customer should be directed to complete a records request.

6. If staff have any concerns surrounding sensitive PII being shared, they must consult with their direct Supervisor.

Acknowledgment:

I, _____, acknowledge that I have read and understand the above policy for handling Personally Identifiable Information and information sharing.