Department of Human Resources 311 West Saratoga Street Baltimore MD 21201	**Family Investment Administration** **ACTION TRANSMITTAL**
Control Number: #11-01	**Effective Date: UPON RECEIPT** **Issuance Date: July 19, 2010**

TO: **DIRECTORS, LOCAL DEPARTMENTS OF SOCIAL SERVICES**
DEPUTY/ASSISTANT DIRECTORS FOR FAMILY INVESTMENT
FAMILY INVESTMENT SUPERVISORS AND ELIGIBILITY STAFF

FROM: **KEVIN M. MCGUIRE, EXECUTIVE DIRECTOR**
CARNITRA WHITE, EXECUTIVE DIRECTOR, SOCIAL SERVICES ADMINISTRATION

RE: **CONFIDENTIALITY AND SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII)**

PROGRAM AFFECTED: **TEMPORARY CASH ASSISTANCE (TCA), TEMPORARY DISABILITY ASSISTANCE PROGRAM (TDAP), PUBLIC ASSISTANCE TO ADULTS (PAA), FOSTER CARE (FC)**

ORIGINATING OFFICE: **OFFICE OF PROGRAMS**

SUMMARY:

The purpose of this Action Transmittal is to provide additional information on the procedures for safeguarding the confidentiality of Interim Assistance Reimbursement (IAR) data, customer personally identifiable information (PII) and the limitations on the use of that data. This AT speaks specifically to IAR information, but is in conjunction with other information on confidentiality and safeguarding information that was previously issued.

IAR information is subject to the Privacy Act, the Federal Information Security Management Act (FISMA) (Public Law 107-347, Title III, section 301) as it applies to the electronic storage, transport of records between agencies, and the internal processing of records received by the state under the terms of its agreement with the Federal government. Federal law (e.g., 42U.S.C. subsection 1306(a), 5 U.S.C. subsections 552 and 552a, and implementing regulations 20 CFR Part 401) further protect IAR data.

All employees must properly safeguard PII furnished by SSA under the IAR agreement from loss, theft or inadvertent disclosure. Employees must understand that they are responsible for safeguarding this information at all times, regardless of whether or not the State employee or the contractor/agent is at his or her regular work site.

SSA at its discretion may conduct onsite inspections to monitor compliance with FISMA regulations.

IAR data includes the:

- Interim Reimbursement Authorization form (DHR/FIA340)
- automated data that the state transmits to Social Security
- notice provided to individuals advising how the SSI reimbursement was calculated
- electronic accounting information SSA sends to the state

Personally Identifiable Information (PII) includes:

- Social Security Number
- Name of individual
- Date of Birth
- Address of individual

ACTION REQUIRED:

Local departments must ensure that the following safeguards are in place:

1. Access to the data will be restricted to only those authorized staff who need it to perform their official duties in connection with the intended use of the data;

2. The data will be stored using a secure Internet process or in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use;

3. The data will be processed under the immediate supervision and control of authorized personnel in a manner which will protect the confidentiality of the data, and in such a way that unauthorized persons cannot retrieve the data by means of computer, remote terminal or other means; and

4. All personnel who have access to the data will be :

    - advised of the confidential nature of the information,
    - the safeguards required to protect the information, and
    - the sanctions for noncompliance with those safeguards

Incident Reporting

All staff must properly safeguard PII from loss, theft or inadvertent disclosure. Employees must understand that they are responsible for safeguarding this information at all times, regardless of whether or not the employee or the contractor/agent is at his or her regular work site.

- All laptops and other electronic devices/media containing PII and used by staff or contractors must be encrypted and/or password protected.

- Email containing PII must only be e-mailed to and from addresses that are secure or encrypted.

- All employees must adhere to these procedures.

- The disclosure of customer information and details relating to a potential or real PII loss is limited to those with a need to know only.

- When an employee becomes aware of the possible or suspected loss of PII, the supervisor and designated local department staff must be notified of the incident immediately.

    - LDSS administrative staff must immediately contact Vesta Kimble at 410-767-7947 or Rosemary Malone at 410-767-7949 or their designees.

    - State staff must notify the SSA regional office contact or if for some other reason, e.g., it is outside the regional office's normal business hours, the State staff must call SSA's Network Customer Service Center (NCSC) at 410-965-7777 or toll free at 1-888-772-6111.

- In the event of a potential or suspected loss, updates must be provided to the SSA using the required Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information (PII) (see attached).

- The State and/or contractor/agent must use the worksheet to quickly gather and organize information about the incident.

ACTION DUE: **Upon receipt**

INQUIRIES: Please direct all TCA inquiries to Marilyn Lorenzo at 410-767-7333 or mlorenzo@dhr.state.md.us or Gretchen Simpson at 410-767-7937 or gsimpson@dhr.state.md.us.

cc: DHR Executive Staff
FIA Management Staff
Constituent Services
DHR Help Desk

Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information (PII)

1. Information about the individual making the report:

Name					
Position					
State Agency/Company					
Phone Numbers					
Work		Cell		Home/Other	
Email Address					
Position Type *(select one)*					
	Management Official		Security Officer		Non-Management

2. Information about the data that was lost/stolen:

Describe what was lost or stolen *(e.g., case file, MBR data)*:

Which element(s) of PII did the data contain?

Name		Bank Account Information	
SSN		Medical/Health Information	
Date of Birth		Benefit Payment Information	
Place of Birth		Mother's Maiden Name	
Address			
Other *(describe)*			
Estimated volume of records involved			

3. How was the data physically stored, packaged and/or contained?

Paper or Electronic *(circle one and continue below)*:

If Electronic, what type of device?

Laptop		Tablet		Backup Tape		Blackberry	
Workstation		Server		CD/DVD		Blackberry Phone #	
Hard Drive		Floppy Disk		USB Drive			
Other *(describe)*							

Additional questions, if electronic:

	Yes	No	Not Sure
a. Was the device encrypted?			
b. Was the device password protected?			
c. If a laptop or tablet, was a VPN SmartCard lost?			
Cardholder's Name			

Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information (PII)

	Cardholder's SSA logon PIN	
	Hardware Make/Model	
	Hardware Serial #	

If Paper:

	Yes	No	Not Sure
a. Was the information in a locked briefcase?			
b. Was the information in a locked cabinet or drawer?			
c. Was the information in a locked vehicle trunk?			
d. Was the information redacted (personal information deleted or blacked out)?			
e. Other *(describe)*			

4. Information about the individual in possession of the data at the time of loss (if same individual as in #1, please indicate "Same as in #1":

Name					
Position					
State Agency/Company					
Phone Numbers:					
Work		Cell		Home/Other	
Email Address					

If person who was in possession of the data or assigned to the data is a contractor employee:

Contractor	
State Agency Contract Identification Number *(if known)*	

5. Circumstances of the loss:

a. When was it lost/stolen?
b. Brief description of how the loss/theft occurred:
c. When was it reported to an SSA management official *(date and time)*?

Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information (PII)

6. Have any other SSA components/individuals been contacted? If so, who? *(include Deputy Commissioner-level, Agency-level, Regional/Associate-level component names)*

Name	SSA Component	Phone Number

7. What reports have been filed? (include local police, and SSA reports)

Report Filed	Yes	No	Report Number
Local Police			
Other *(describe)*			