Operations Memorandum
Cash
SNAP
Medicaid
OPS-13-01-04

January 29, 2013

SUBJECT: **Internal Revenue Service (IRS) Income Eligibility Verification System (IEVS) Safeguarding Requirements**
TO: **Executive Directors**
FROM: **Richard Wallace,Acting Director, Bureau of Operations**

Purpose

To provide County Assistance Offices (CAOs) with guidance on IRS IEVS Safeguarding Requirements. This Operations Memorandum supersedes OPS 050903

Background/Discussion

The Taxpayer Browsing Protection Act requires that security measures be taken to prevent the release of individual taxpayer information. CAO workers are required to complete the safeguarding IEVS training annually. Safeguarding IEVS e-learning training clarifies the requirements for disclosure and handling of information received from the IRS. These IRS safeguarding requirements and disclosure restrictions are also accessible in Supplemental Handbook Chapter 930 Section 930.61, *Tax Information Safeguards and Penalties;* and in Using IEVS, Chapter 1, General Information, *Verifying IRS Information*.

The IRS mandates that all employees be notified annually of the following criminal penalties associated with unauthorized use of IRS information:

Unauthorized disclosure of federal tax information is a crime punishable by a $5,000 fine and immediate action to ensure compliance and/or five years imprisonment; and Unauthorized inspection of federal tax information is a crime punishable by a $1,000 fine and/or one year imprisonment (26 U.S.C. §§ 7213 and 7213A).

The Department of Public Welfare (DPW) Office of General Counsel (OGC) clarified that, for Federal tax return and Federal Tax Information (FTI) to be protected under federal income tax law, the return information must be filed with, received by, recorded by, prepared by, furnished to, or collected by the IRS and then shared with DPW. If the information comes from another source (such as a bank, the applicant, employer, etc.) directly to the CAO, it is not FTI and does not have to be protected and

segregated from other information in the case record or system beyond regular program requirements.

For example, if the client provides a 1040 tax return or other tax forms to the CAO, it is not considered FTI, but it can be scanned and made part of the case record the same as other types of verification documents provided by the client.

PROCEDURES:

CAOs must comply with the following:

1. Financial information obtained via IEVS IRS Exchanges 4 and 5 must not be printed.

   - IEVS IRS "hits" information is to be narrated in the case record as an IEVS "hit" without stating that the source of the information is IRS Exchange 4 or 5.

2. The PA 189 Overpayment and Referral Data Input form, which is used to track the PA 76 Request for Financial Information and the PA 78 Request for Employment Information in Automated Restitution Referral and Computation (ARRC), shall only contain the following information:

   - Caseload number
   - Worker ID
   - Case name
   - Case record number
   - Date of discovery
   - Reason code
   - Whether a PA 76/PA 78 was sent and the date

   Any information found on IEVS Exchanges 4 and 5 that is not known from the case record or not given to the CAO by the client can be FTI. The CAO **must not** write any FTI on the PA 76 or PA 78 when sending requests out, or when requests for FTI information are returned, because the forms would then become forms with confidential FTI and must be protected and segregated under federal law.

   However, any information written on the PA 76 or PA 78 by the employer, bank or other institution or source and then returned to the CAO is not FTI.

3. Staff inputting requests for IEVS financial information must be instructed to ensure that IEVS data exchange information is used only to obtain information about applicants, recipients, and individuals whose income and resources must be considered to determine eligibility or the amount of the benefit. This includes Legally Responsible Relatives of the applicant and/or recipient.

4. Any employee observing improper disclosure or inspection of IRS information must report it to their Executive Director or their designee, who, in turn, will complete the IT

Security Incident Reporting form and submit it to DPW's CISO at ra-itsecurity@state.pa.us or fax to 717-772-7163.

Provide the following information:

- Date and time of the incident
- Date and time the incident was discovered
- How the incident was discovered
- Description of the incident and the data involved. Include specific data elements if known, including whether the information was encrypted or protected by other means.
- Potential number of sensitive data records involved. If unknown, provide a range if possible
- Location where the incident occurred
- Information technology involved (e.g., workstation, laptop, server, mainframe)

5. Access to IEVS IRS Exchange 4 and 5 is restricted as follows:

- Inquiry access to IEVS IRS Exchange 4 and 5 is restricted to Income Maintenance Caseworkers (IMCWs), IMCW supervisors, CAO Managers and Executive Directors only, since this information is confidential and is needed in the eligibility determination process.
- Requests for inquiry access to IEVS Exchanges 4 and 5 by staff other than listed above must to be approved via request to the Area Manager. The CAO will be notified if the request is approved and if access is granted.

6. Further Instructions for Exchanges 4 and 5:

- If information from Exchanges 4 and 5 are printed in error, the printouts must be destroyed. A destruction log must be kept and maintained for five years. This log must include the date that IEVS printouts of FTI were destroyed and method of destruction, etc. (**IRS Pub 1075, Section 3.2 and Section 3.3**).

NOTE: The **PA 1885** IEVS Destruction Log for FTI is available on DocuShare.

- FTI furnished to the user and any paper material generated from it, such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes, and work papers must be also be destroyed. Shredding is the preferred method of destruction. If any IEVS Exchanges 4 or 5 prints are received from another CAO or agency, it should be reported to your supervisor. The sending office should be notified of the violation and the receiving office must shred the Exchanges 4 or 5 prints and log the information on their destruction log.
- The destruction log must be maintained by each office, even if no items are destroyed.
- Destruction of FTI should be witnessed by an agency employee (**IRS Pub 1075, Section 8.4**).

- The following precautions must be observed when shredding/destroying FTI:

  To make reconstruction more difficult, the paper must be inserted so that lines of print are perpendicular to the cutting line. The paper must be shredded to effect 5/16 inch wide or smaller strips; microfilm and microfiche must be shredded to effect 1/35 inch by 3/8 inch strips. If shredding is part of the overall destruction of FTI, strips can, in effect, be set at the industry standard (currently 1/2 inch). However, when deviating from IRS's 5/16 inch requirement, FTI, as long as it is in this condition (i.e., strips larger than 5/16 inch), must be safeguarded until it reaches the stage where it is rendered unreadable.

7. The e-Learning IRS IEVS Safeguarding training must be completed annually by all OIM staff. Upon completion of the training, OIM workers are to:

   - Complete the registration form
   - Print the Training Completion Form and IRS User Agreement
   - Sign the IRS User Agreement form and give both forms to his/her supervisor to log

   NOTE: Printing the Training Completion form includes the statement "This training included notification of Internal Revenue Code Section 7213, 7213 A and 7431, which state unauthorized disclosure of information, returns or return information and unauthorized inspection of returns or return information is a crime punishable by a $5,000 fine and/or five years in prison." This statement of the Training Completion Form is to ensure compliance with the IRS safeguarding tax information requirements.

8. Periodic internal inspections will be conducted in accordance with IRS Tax Information Security Guidelines for Federal, State, and Local Agencies to ensure that safeguards are adequate. **CAOs will be reviewed every three years. Headquarters units will be reviewed every 18 months.**

NEXT STEPS

1. Share and review this information with all members of your staff.

2. Refer any questions to your area manager.