5101:9-9-25 **Federal tax return information safeguarding procedures.**

(A) Safeguarding procedures for the income eligibility verification system (IEVS),and the treasury offset program (TOP), ~~and the treasury offset program~~ are necessary to ensure the confidential relationship between the taxpayer and the internal revenue service (IRS). Safeguarding of federal tax information received by the CDJFS is required. Safeguarding procedures are derived from the "Tax Information Security Guidelines" booklet, "IRS Publication 1075," prepared by the IRS and from the September 1991 IRS "Safeguard Review Report."

(B) Disclosure of tax return information to federal, state and local agencies by the IRS or the social security administration (SSA) for use in their TANF, medicaid, and food stamp programs is authorized by internal revenue code. Federal tax information (FTI) for IEVS is disclosed solely for the purpose of determining eligibility or the correct amount of benefits for each program , and is information from federal wage or IRS matches. FTI for ~~FTROP~~ TOP is disclosed to specific county staff for administrative purposes. FTI disclosed for TOP ~~and the federal salary offset program~~ are the names of the individuals whose social security numbers have matched~~, and~~ the amount of the tax ~~or salary~~ refund offset, and the most recent IRS address for each matched individual.

(C) The IRS conducts on-site reviews of safeguards at least once every five years, and recommends that periodic inspections should be conducted during the year to ascertain that safeguards are adequate. ODJFS staff will inspect each CDJFS ~~not less than once per year~~ within a three year cycle, to ascertain that safeguards of federal tax information disclosed per paragraph (B) of this rule are adequate. ODJFS reviewers will review a sample of case records, client registration information system-enhanced (CRIS-E) running ~~review a sample of case records, client registration information system-enhanced (CRIS-E) running~~ record comments~~.~~, and general safeguarding procedures for possible safeguarding violations of FTI.

A record will be made of each inspection, citing the findings (deficiencies) as well as recommendations and corrective actions taken where appropriate. CDJFS have forty-five days from the date they are notified of the deficiencies to correct these deficiencies.

(D) CDJFS must have written procedures governing the security of federal tax return information. These procedures must include employee awareness, storage and handling, access, facility security and disposal as addressed in paragraphs (E) to (J) of this rule. ODJFS staff will review these procedures for compliance with the "Tax Information Security Guidelines" and ODJFS safeguard requirements. The written procedures must be updated periodically to reflect significant program changes.

(E) Employees must be advised at least annually that unauthorized disclosure of FTI is a

crime that may be punishable by a five thousand dollar fine, five years imprisonment, or both. Employees must also be advised annually that a taxpayer may bring suit for civil damages in a United States district court for unauthorized disclosure of returns and return information. There are punitive damages in case of willful disclosure or gross negligence, as well as the cost of the action.

Employees should be made aware that these civil and criminal penalties apply even if the unauthorized disclosure was made after their employment with the CDJFS terminated. Employees should also be briefed annually on FTI security procedures.

(F) FTI should be handled in such a manner that it does not become misplaced or available to unauthorized staff. Confidential federal tax information must be placed either in a locked container or in locked desks when not in use. Further information on locked containers is included in IRS Publication 1075, "Tax Information Security Guidelines."

The two major types of locking devices are key locks and combination locks. Combinations to locks must be changed when any of the following conditions exist:

(1) When the safe or lock is originally received,

(2) At least once a year,

(3) When an employee who knows the combination leaves, or

(4) Whenever the combination is compromised in any way.

Keys should ~~only~~ be issued only to persons needing to access the files and duplicate keys should be kept to a minimum.

(G) FTI file storage areas require more than normal security. Access to these areas must be limited to the absolute minimum number of employees necessary. The following principles should be followed to adequately restrict access to the files area.

(1) There should be written procedures identifying employees who have access to FTI.

(2) Signs must be posted to restrict access.

(3) Cleaning must be performed in the presence of a secured employee.

(4) Personnel identification system is recommended in all locations where files

contain FTI.

(5) Access to file areas which contain FTI must be restricted to workers who have a security profile.

(6) The location and physical layout of the files area should be such that unnecessary traffic is avoided.

(7) A sign in/out register should be maintained.

(8) Keys to the files must ~~only~~ be issued only to persons authorized to enter area.

(H) FTI must be handled in such a manner that it does not become misplaced or available to unauthorized personnel. Good safeguarding practice is that access to FTI must be strictly on a need-to-know basis. The potential for improper disclosure is minimized by restricting access to designated personnel. Staff must not be given more information than needed to do their work.

(1) Any FTI which is provided through CRIS-E or on paper must not be commingled with other information.

(2) FTI should not be filed in areas used for breaks, food preparation or any similar facilities which would be used by employees not authorized to have access to FTI. FTI files must not be maintained in areas that allow clients access.

(I) If possible, security staff should be CDJFS employees. Only authorized employees can have access to areas with FTI during nonworking hours.

(J) There must not be any FTI in case records, open or closed, that is not safeguarded. Federal tax information must not be on the CRIS-E running records. FTI must not be on the comments or any other screen that can be accessed by persons not connected to the case through inquiry on a need-to-know basis.

Replaces: 5101-9-25

Effective: 05/23/2003

CERTIFIED ELECTRONICALLY

Certification

05/13/2003

Date

Promulgated Under: 111.15
Statutory Authority: 5101.02
Rule Amplifies: 5101.02, 329.04
Prior Effective Dates: 5/1/93, 9/27/93, 6/26/95, 2/15/96, 11/1/96, 10/4/2002.