

DMA ADMINISTRATIVE LETTER NO. No. 16-02

DSS ADMINISTRATIVE LETTER NO. ECONOMIC INDEPENDENCE(WORK FIRST AND FOOD STAMPS) 04-2002

**DSS ADMINISTRATIVE LETTER NO. ADULT AND FAMILY SERVICES
02-2002**

TO: COUNTY DIRECTORS

ATTENTION: INCOME MAINTENANCE DIRECTORS

MEDICAID CASEWORKERS AND SUPERVISORS

WORK FIRST CASEWORKERS AND SUPERVISORS

FOOD STAMP CASEWORKERS AND SUPERVISORS

SPECIAL ASSISTANCE CASEWORKERS AND SUPERVISORS

SECURITY CONTROL OFFICERS

FRR/BEER CONTROL OFFICERS

DATE: MARCH 11, 2002

SUBJECT: SECURITY OF INTERNAL REVENUE SERVICE AND

SOCIAL SECURITY ADMINISTRATION INFORMATION

NOTE: This letter obsoletes DSS Administrative Letter No. Economic Independence (Work First and Food Stamps) 11-2000, DSS Administrative Letter No. Adult and Family Services 3-2000, and DMA Administrative Letter No. 30-2000. The letter is effective upon receipt.

The purpose of this letter is to provide you with updated information concerning the security requirements for IRS and SSA data.

The changes include a revised Documentation of Annual Security Training log, a sample log of who has accessed FRR/BEER reports, a sample FRR/BEER destruction log, new requirements for two levels of security within the building where IRS and SSA data are stored, and additional instructions regarding who completes the internal inspection audit. The time limit for retaining the log for access to the FRR/BEER and the FRR/BEER destruction log has changed to five years. Revisions are in **bold** print in the paper version and red in the online version throughout the letter.

I. BACKGROUND

The Income and Eligibility Verification System (IEVS) was implemented in October 1986. This system provided a mechanism to interface with the Internal Revenue Service (IRS) to obtain leads regarding income and resources reported to the IRS by employers and financial institutions. This matched information is printed on the Financial Resource Report (FRR). IEVS also gave us access to certain types of income reported to SSA by the IRS. These income types are: military employment, pension income, self-employment, and federal employment. This matched information is printed on the Beneficiary Earnings Exchange Report (BEER).

The matches with SSA are also regulated by IEVS. These matches are the State Data Exchange (SDX), Beneficiary Data Exchange (BENDEX), State Online Query (SOLQ), and the Third Party Query (TPQY). Also, to ensure that we have the correct social security number (SSN) when performing these matches, we submit records to SSA for SSN validation.

DHHS contracts with the IRS and SSA to perform these matches. In these contracts, DHHS agrees to safeguard the information provided to us in accordance with federal regulations. IRS security requirements are defined in 26 USC 6103 and IRS Publication 1075. SSA security requirements are defined in: Section 1106(a) of the Social Security Act (42 USC 1306(a)); SSA POMS 10801.500, 510, 515, and 828; Regulation No. 1 (20 CFR Part 401); the Privacy Act (5 USC 552a); Freedom of Information Act (5 USC 552); Computer Matching and Privacy Protection Act of 1988 (PL 100-503); 26 USC 6103, and IRS Publication 1075.

II. RESPONSIBILITIES OF THE COUNTY DIRECTOR

A. The director appoints the FRR/BEER control person and a back up FRR/BEER control person.

B. The director also designates who is responsible for providing training and annual review of the policies on security procedures. The following requirements must be met.

1. All agency employees having access to Federal tax information must be thoroughly briefed on security procedures and instructions requiring their awareness and compliance. This includes cleaning staff, security staff, mail handlers, and any other individuals who have access to this data because of their job responsibilities.

2. Give copies of Internal Revenue Code Sections 7213(a), 7213A, and 7431 to each new employee when the training is completed. (See [Attachment II](#) for copies of these sections.) Conduct annual

reviews of these procedures for all other employees. Upon the request of the IRS, we have revised the form that is used to track security training. (See [Attachment III](#).) Make a copy of new [Attachment III](#) and ensure that each person attending your annual security training signs the form. Discard all previous versions of the training log.

C. The director ensures security requirements are met for the agency. The IRS requires two barriers to accessing federal tax information (FTI) – secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. The FRR/BEER reports contain FTI; therefore, the agency must meet these IRS security requirements. Details of the security requirements are contained in IRS Publication 1075. This publication can be accessed through the Internet. Go to: <ftp://ftp.fedworld.gov/pub/irs-pdf/p1075.pdf>. Section 4.0 contains the security information. If your agency does not have access to the Internet, you may contact Ken Maddox, the IEVS coordinator, at (919) 857-4019 with questions or information needed regarding the security requirements.

III. RESPONSIBILITIES OF THE FRR/BEER CONTROL PERSON

The FRR/BEER are mailed to the counties in hot pink envelopes and marked “Confidential”. These reports must NOT be opened in the mailroom, but must be delivered to the designated FRR/BEER control person. Immediately upon receipt, the control person must distribute the workers’ copies to the appropriate income maintenance staff for follow-up. To ensure that only individuals who are allowed access to this information handle these reports, the control person must keep a log indicating to whom the reports are given, the date signed out, and the date the information is returned. See [Attachment IV](#) for a sample log. When worker copies are distributed, record the names of the staff members who received the copies on a log. Also record on the log the names of any other persons who view the FRR/BEER information. Retain this log for five years, at which time it may be destroyed.

The control person must also ensure that the reports are under lock and key when they are not being used by the workers, the reports are worked within the time frame specified in the appropriate program policy manual, and that all worker copies of the report are returned and filed with the control copy. Do not destroy a FRR/BEER report until all copies of the report are returned.

IV. RESPONSIBILITIES OF THE INCOME MAINTENANCE CASEWORKER

A. The Income Maintenance Caseworker must safeguard the FRR and BEER while he is using the reports. If the worker leaves the office before

he has completed using the report, he must lock the report in a file cabinet or drawer, or lock his office door. If the worker does not have a lock available, he must return the reports to the control person when he leaves the office. If the worker's supervisor has a locking file cabinet or drawer, the worker may give the report to the supervisor to safeguard until his return. All IRS data must be kept out of public view and protected from unauthorized disclosure at all times.

B. Each program policy manual specifies the time frames in which the caseworker must initiate follow-up. Please refer to the Automated Match and Inquiry Sections of the appropriate program policy manual.

C. When the caseworker determines that there are resources or income reported on the FRR or BEER, he must independently verify these resources or income. Follow the steps outlined below when working the FRR or BEER.

1. The caseworker must check the case record to see if this resource or income has been previously reported. If the resource or income has not been previously reported, attempt to obtain the information from the client. Send a letter (See [Attachment VI](#) for a sample.) to the client requesting that he provide the name of the financial institution and the account number. Do not include the name of the institution or account number in this letter.

- a. If the client provides the name of the institution and the account number, document the case record that the client provided this information. The source of the information is no longer the FRR or BEER. Attempt to obtain a signed DSS-3431.

- (1) If the client signs a DSS-3431, send the request for verification of the income or resource to the institution.

- (a) The copy of the verification letter may remain in the case file.

- (b) When the verification letter is returned, file the verification letter in the case record.

- (2) If the client refuses to sign the DSS-3431, propose termination.

- (3) Document the results of the match on the FRR or BEER and return it to the control person.

b. If the client does not respond to the letter or refuses to provide the name of the institution from which he receives income or resources, fill in the financial institution and account number on a DSS-3431 and attempt to obtain the client's signature.

(1) If the client signs the DSS-3431, send the request for verification of the income or resources to the institution.

(a) The copy of the verification letter must be filed with the FRR or BEER.

(b) When the verification letter is returned, file the verification letter with the FRR or BEER. Destroy the copy using procedures in VIII. A. below.

(c) Document in the record by the appropriate resource or income the amount of the resource or income and that verification is filed with the FRR or BEER dated MM/DD/CCYY. Do not document the name of the institution or account number in this record.

(2) If the client refuses to sign the DSS-3431, propose termination.

(3) Document the results of the match on the FRR or BEER and return it to the control person.

2. If the income or resource is documented in the record and was previously verified as terminated, no further verification is required. Document on the FRR or BEER that the information matched what was in the record, and return the reports to the control person.

3. If the income or resource is documented in the record and was previously verified as active, do the following.

a. If the record indicates that the client previously reported this resource or income, document on the FRR or BEER that the information matched what was in the record. You do not need to re-verify this information until the next redetermination or recertification.

(1) At redetermination or recertification, send a request for verification of the income or resource to the institution, using the current DSS-3431. (Refer to

the appropriate program policy manual for the definition of a current DSS-3431.)

(2) The copy of the verification letter may remain in the case file.

(3) When the verification letter is returned, file the verification letter in the case record.

b. If the record indicates that this resource or income was originally obtained from the FRR or BEER, document on the FRR or BEER that the information matched what was in the record. You do not need to re-verify this information until the next redetermination or recertification.

(1) At redetermination or recertification, send a request for verification to the institution, using a current DSS-3431.

(2) The copy of the verification letter must be filed with the FRR or BEER.

(3) When the verification letter is returned, file the verification letter with the FRR or BEER. Destroy the copy using procedures in VIII. A.

(4) Document in the record by the appropriate resource or income the amount of the resource or income and that the verification is filed with the FRR or BEER dated MM/DD/CCYY.

NOTE: If the record indicates that the information was information never changes. All subsequent verifications of this information must be filed with the FRR or BEER.

D. You may tell the individual who has resources reported on the FRR or someone acting as his representative that you obtained the information from the Internal Revenue Service and you may disclose the information that was printed on the FRR.

E. If the client is determined to be ineligible based on verification obtained as a result of information on the FRR, propose termination using the verified information.

V. RESPONSIBILITIES OF THE MEDICAID PROGRAM REPRESENTATIVES

The Medicaid Program Representative (MPR) is responsible for the following:

A. Reviewing security procedures in your county and completing the Report of Internal Inspection ([Attachment I](#)). As a part of this review, the MPR will request you to provide the signed security training forms.

B. Notifying the county director of any deficiencies found.

C. Requesting a Corrective Action Plan from your county for any deficiencies found during the review of the security procedures.

D. Working with your county to resolve the problems with Medicaid if any shortcomings are found in the annual review.

E. Notifying all other Program Representatives who will be responsible for working with the county to resolve the problems with their assigned programs.

F. Submitting the Report of Internal Inspection and the signed security training forms to DMA.

VI. OTHER DISCLOSURE RULES

If you are investigating for an overpayment or you prosecute for fraud, you may use the verification, but you cannot state that this information was obtained from the IRS to the individuals (other than the client) involved in the case. You can only state that you have verified this information with the source (the financial institution).

VII. RETENTION OF THE FRR AND BEER

Maintain the FRR and BEER in the county for two years, unless there is a current fraud case. The FRR or BEER related to that case should be flagged for retention. The FRR and BEER information is retained in the State Office for three years. If information between the second and third year is needed for audit purposes, please contact the IEVS Coordinator.

VIII. DESTRUCTION

A. The FRR, BEER, and information obtained from these reports can be destroyed after two years (if all copies returned) by one of the following methods:

1. Incineration: You must ensure that all pages are consumed.
2. Shredding: To make reconstruction difficult, the paper should be inserted so that lines are perpendicular to the cutting line. The paper must be shredded into strips that are no wider than 5/16-inch.
3. Microfilmed data must be incinerated or melted, or shredded to a 1/35-inch by 3/8-inch strip.

A log listing the dates the FRR and BEER reports were destroyed and the dates of the reports that were destroyed is required. See [Attachment V](#) for a sample log to record information when you destroy FRR and BEER reports. Retain this log for five years.

B. SSA data (SDX, BENDEX, SOLQ, and TPQY) can be destroyed after three years, or after all audits have cleared, by one of the following methods:

1. Shredding
2. Incineration
3. Sealing the material in cardboard boxes and burying at a landfill under management supervision.
4. Microfilmed data must be incinerated or melted, or shredded to a 1/35-inch by 3/8-inch strip.

IX. OTHER SECURITY MEASURES

A. When microfilming or imaging case information, this data should be treated with the same security measures as case records.

B. Store screen prints of TPQY, SDX, BENDEX, SOLQ, SDX and BENDEX sheets in an area that is physically safe from access by unauthorized individuals during normal business

hours as well as non-business hours, such as in a locked metal file cabinet, locked desk, or in a locked office.

C. If screen prints are routed to a shared printer in a common area, retrieve screen prints immediately. This is especially important if the printer is located in a hallway through which visitors pass.

D. Information obtained from the FRR/BEER cannot be transmitted via email.

If you have any questions regarding this information, please contact your Medicaid Program Representative.

Sincerely,

Nina M. Yeager, Director

Division of Medical
Assistance

Pheon Beal, Director

Division of Social Services

(This material was researched and prepared by Mary Spivey, EIS Program Consultant, DMA/EIS Unit.)