SECURITY OF INTERNAL REVENUE SERVICE AND SOCIAL SECURITY ADMINISTRATION INFORMATION

EFFECTIVE 8/15/2023 - CHANGE NO. 11-23

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 Social Security of Administration (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 the local agency has the correct social security number (SSN) when performing these matches, the records are submitted to SSA for SSN validation. Department of Health and Human Services (DHHS) contracts with the IRS and SSA to perform these matches. In these contracts, DHHS agrees to safeguard the information provided to the local agency 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));
- Regulation No. 1 (20 CFR Part 401);
- 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 301.6103; and
- IRS Publication 1075.

II. RESPONSIBILITIES OF THE COUNTY DIRECTOR

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

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 (FTI) must complete the Safeguard Awareness Training which can be found in the NC FAST Learning Gateway: **FRR-BEER Safeguard Awareness Training. Each employee and new hires must** be thoroughly briefed on security procedures and instructions requiring their awareness and compliance. This includes cleaning, maintenance, and Security staff, and any other individuals who have access to this data because of their job responsibilities**.**

   Those employees granted access to FTI must complete a background investigation. The background investigation must include, at minimum:

   a. Requires FBI Fingerprinting (FD-258)
   b. Local Law Checks
   c. Citizenship/Residency Status

   Reinvestigation requirements have been changed from being conducted every 10 years to every 5 years.

2. Provide copies of Internal Revenue Code Sections 7213(a), 7213A, and 7431 to each new employee when the training is completed. Review IRC Rules Handout DHB-2194, IRC Rules Handout for copies of these sections.

3. Conduct annual reviews of these procedures (Annual Safeguard Awareness Training) for all other employees.

4. Review DHB-2201, Confidentiality Form.

5. Ensure each staff person attending the annual security training signs and date(s) the DHB – 2195, Documentation of Annual Security Training. This includes new hires beginning employment with the Agency, or when staff job changes require access to FTI.

6. Discard all outdated previous versions of the training logs, only use the current revised logs.

C. The director ensures security requirements are met for the agency. The IRS requires staff that handle federal tax information (FTI) have background check performed on them and 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: http://www.irs.gov/pub/irs-pdf/p1075.pdf.

III. RESPONSIBILITIES OF THE FRR/BEER CONTROL PERSON

The FRR/BEER reports are posted online in NCXCloud and XPTR for the counties, which are accessed by the control officers in the county department of social services (dss). Immediately upon receipt, the control officers must distribute the workers' copies to the appropriate caseworkers 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. Refer to DHB-2197, FTI Record Keeping Log for a sample log. When caseworker 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 officers must also ensure that the reports are under lock and key when they are not being used by the caseworkers, the reports are worked within the time frame specified in the appropriate program policy manual, and that all caseworker copies of the report are returned and filed with the control copy. When filing FTI in cabinets or on the computer, all FTI must be labeled as such, not FRR or BEER, but FTI. **Do not destroy FRR/BEER reports until all copies of the report are returned.**

To access NCXCloud (Scroll to the bottom of this site to where it says: User Training and Resources)
https://itservices.nc.gov/services/data-analytics/ncxcloud#UserTrainingResources-626

IV. RESPONSIBILITIES OF THE CASEWORKER

A. Caseworker Responsibility

The caseworker must safeguard the FRR and BEER reports while they are being used. If the caseworker leaves the office before they have completed using the report, they must lock the report in a file cabinet or drawer or lock their office door.

If the caseworker does not have a lock available, then they must return the reports to the control person when they leave the office. If the caseworker's supervisor has a

locking file cabinet or drawer, the caseworker may give the report to the supervisor to safeguard until they return.

All IRS data must always be kept out of public view and protected from unauthorized disclosure.

B. Initiate Follow-up

Each program policy manual specifies the time frames in which the caseworker must initiate follow-up. Please refer to the MA-2430/3515 Automated Inquiry and Match Procedures sections of the appropriate program policy manual.

C. Reported Resources or Income

When the caseworker determines that there are resources or income reportedon the FRR or BEER, they must independently verify these resources or income. Follow the steps outlined below when working on 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 beneficiary. Send a letter (See **DHB -2202, Beneficiary Notice** for a sample) to the beneficiary 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 beneficiary provides the name of the institution and the account number, document the case record that the beneficiary 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 beneficiary signs a DSS-3431, send the request for verification of the income or resource to the institution.

            (a) A 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 beneficiary 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 beneficiary does not respond to the letter or refuses to provide the

name of the institution from which they receive income or resources, fill in the financial institution and account number on a DSS-3431 and attempt to obtain the beneficiary's signature.

(1) If the beneficiary 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 IX. 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 <u>not</u> document the name of the institution or account number in this record.**

(2) If the beneficiary 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 beneficiary previously reported this resource or income, document on the FRR or BEER that the information matched what was in the record. The caseworker does not need to re-verify this information until the next recertification.

(1) At 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) A 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. Caseworker does not need to re-verify this information until the next recertification.

(1) At recertification, send a request forverification 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 IX.

(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.

(5) If the record indicates that the information was originally obtained from the FRR or BEER, the source of this information never changes. All subsequent verifications of this information mustbe filed with the FRR or BEER.

D. The caseworker may tell the beneficiary and/or authorized representative who has resources reported on the FRR, that the caseworker obtained the information from the Internal Revenue Service. The caseworker may disclose the information that was printed on the FRR.

E. If the beneficiary 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 OPERATIONAL SUPPORT TEAM (OST)

A. Review the DHB-2190, Report of Internal Inspection completed by the local agency every 3 years with the agency Security Officer. OST will affirm that what the local agency reports on the Internal Inspection is accurate and provide the signed DHB 2190 to the IEVS Coordinator.

B. Notify the county director of any deficiencies found by the IEVS Coordinator on

the Plan of Action and Milestones (POAM).

C. Request a Corrective Action Plan from the local agency for any deficiencies found during the review of the security procedures.

D. Work with the local agency to resolve the problems with Medicaid if any shortcomings are found in the Internal Inspection.

VI. OTHER DISCLOSURE RULES

If the caseworker is investigating for an overpayment or prosecution for fraud, the caseworker may use the verification, but the caseworker **cannot** state that this information was obtained from the IRS to the beneficiary involved in the case. The caseworker can only state that they have verified this information with the source (the financial institution).

Disclosure of FTI to state auditors by child support enforcement and human services agencies is not authorized by statute. FTI in case files must be removed prior to access by the auditors.

VII. UNAUTHORIZED DISCLOSURE AND INCIDENTS

Refer to DHB-2194 IRC Rules Handout.

VIII. RETENTION OF THE FRR/BEER AND RECORD LOGS

Maintain the FRR and BEER at the local agency for five years unless there is a current fraud case. The FRR or BEER related to that case should be flagged for retention. If a county needs copies of the FRR/ or BEER reports from previous years, please contact the IEVS Coordinator.

All record logs must be maintained for five years.

IX. DESTRUCTION

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

1. Burning: The material must be burned in an incinerator that produces enough heat to burn the entire bundle, or the bundle must be separated to ensure that all pages are incinerated.

2. Shredding: To make reconstruction difficult, destroy paper using crosscut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in

size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen.

3. Electronic media (e.g., hard drives, tapes, CDs and flash media) containing FTI must not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape must be destroyed by burning or shredding in accordance with applicable standards.

4. Destroy microfilms (microfilm, microfiche, or other reduced image photo negatives) by burning. (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 is required. Refer to DHB-2198, Destruction Log for FRR/BEER for a sample log to record information when to 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 outlined in IX.A above.

X. 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, SOLQI, 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 or fax.

The local agencies that receive FTI under authority of IRC 6103(l)(7) (human services agencies) may not disclose FTI to contractors for any purpose.

XI. EMAIL COMMUNICATION AND FAX EQUIPMENT

A. FTI is prohibited in email transmissions outside of the agency's internal network**.**

If FTI has been included in emails or email attachments, the agency must only transmit FTI to an authorized recipient and must adhere to the following requirement:

1. FTI must be properly protected and secured when being transmitted via email.

2. Mail servers and clients must be securely configured. Underlying operating systems of on premises mail servers must be hardened and included in the agency's FTI inventory. A 45-day cloud notification must be submitted for cloud-hosted mail solutions.

3. The network infrastructure must be securely configured to block unauthorized traffic, limit security vulnerabilities, and provide an additional security layer to an agency's mail servers and clients.

4. Emails that contain FTI should be properly labeled (e.g., email subject contains("FTI") to ensure that the recipient is aware that the message content contains FTI.

5. Audit logging must be implemented to track all sent and received emails containing FTI.

6. Email transmissions that contain FTI must be encrypted using a FIPS 140 validated mechanism.

7. Malware protection must be implemented at one or more points within the email delivery process to protect against viruses, worms, and other forms of malware.

B. FTI is <u>prohibited</u> from inclusion with fax communications. If Federal Tax Information (FTI) is included within a fax communication, the agency must transmit to an authorized recipient and adhere to the following requirements:

1. Have a trusted staff member at both the sending and receiving fax machines.

2. Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI.

3. Place fax machines in a secure area.

4. Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes:

   a. A notification of the sensitivity of the data and the need for protection

   b. A notice to unintended recipients to telephone the sender—collect, if

Necessary, to report the disclosure and confirm destruction of the information.

If digital fax servers are used, they should be hardened like other servers containing FTI.

XII. FRR/BEER SAFEGUARDING ALTERNATE WORK SITE

If the confidentiality of FTI can be adequately protected, alternative work sites, such as employee's home or other non-traditional work sites can be used despite the location. FTI remains subject to the same safeguard requirements and the highest level of attainable security.

XIII. BADGES AND VISITORS FOR FACILITIES WITH FTI

A. ID Badge

All NC FAST and DHB staff shall have at least 2 badges: 1 white badge for RTP building access, and 1 DHHS picture ID badge. The DHHS picture ID badge may also have Broughton and/or McBryde building access if needed. Building and/or cleaning/maintenance staff have their own badges/keys to enter the buildings and offices. NC FAST staff will not allow them into the buildings or offices. Cleaning staff wear uniforms and are clearly identifiable.

B. Staff should follow the security of the building:

Staff MUST wear your DHHS picture ID badge **AT ALL TIMES,** and it must be easily visible.

1. You must show your badge if requested for security reasons.

2. You must not share any of your badges with others, nor allow them to enter secured space (elevators, doors, etc.) with your badge. Everyone must always swipe their own badge for their own entry at all times.

3. If you lose or forget to bring any of your badges, contact Program Support immediately.

4. Do not allow visitors or people you do not recognize into the building; escort them to the Receptionist.

5. Receptionist must not allow anyone they do not recognize or unauthorized staff to go past the reception area.

All local agencies shall follow the Visitor and Badge Policy for their local agency.

XIV. CONTROL AND SAFEGUARDING KEYS AND COMBINATIONS

All containers, rooms, buildings, and facilities containing FTI must be locked when not in actual use. Access to a locked area, room, or container can be controlled only if the key or combination is controlled. Compromising a combination or losing a key negates the security provided by that lock. Combinations to locks must be changed annually or when an employee who knows the combination retires, terminates employment or transfers to another position.

XV. INTERNAL INSPECTION

County agencies are required to conduct internal inspections as part of their compliance with IRS 1075 Publication. The internal inspection report serves as a checklist to identify security procedures and federal security implementation for protecting Federal Tax Information (FTI). The Internal Inspection shall be conducted **every three years.** This is usually completed by the Security Officer in the local agency along with the assistance of OST and the County's Technical staff.

A. Internal Inspection process steps below.

All Counties must complete the Internal Inspections once every three years. The IEVS Coordinator determines when each county completes their Internal Inspections. View the Internal Inspection Schedule here.

1. Complete the Internal Inspection Report. All parties must sign the completed Internal Inspection.

    a. Official Conducting Internal Inspection: Local Agency Security Officer

    b. Head of Location Being Reviewed: Director of the Local Agency

    c. Agency Reviewer: Operational Support Team

2. Complete each field with a Pass, Fail or N/A.

3. A Plan of Action and Milestones (POAM) is created by the State IEVS Coordinator as a result of the findings.

B. Forms required to complete the Internal Inspection can be found on the NCDHSS Policies and Manuals website.

- DHB-2190 - Internal Inspection Report
- DHB-2191 - Designation of control Officer for FRR/BEER Reports
- DHB-2192 - Documentation of Social Security Administration Security Training (Annual Inspection)

- DHB-2194 - IRC Rules Handout
- DHB-2195 - Documentation of Annual Security Training– County Staff
- DHB-2196 - Documentation of Annual Security Training – Shred contractor Training
- DHB-2197 - FTI Record Keeping Log
- DHB-2198 - Log for Destruction of the FRR/BEER Reports
- DHB-2199 - Documentation for the Visitation Log
- DHB-2200 - Access Control Log
- DHB-2201 - Confidentiality of Safeguard Data
- Acceptable Use Policy verification

C. Acceptable Use Policy

All staff are required to view the acceptable use policy, sign and date the last page of the document and include it with the Internal Inspection Report. Email the report to the DHB IEVS Coordinator listed on the communication that is sent out to the counties about the Internal Inspections

D. The IEVS Coordinator reviews the County's Internal Inspection Reports. All findings are listed on the POAM with the documented expected resolution date. The Director and OST will work together to resolve the findings.