TEXAS
Health and Human Services

Cecile Erwin Young
Executive Commissioner

MEPD and TW Bulletin 23-16

Date: Dec. 1, 2023

To: Eligibility Services Supervisors and Staff
Program Managers
Regional Directors
Regional Attorneys
Hearings Officers

From: Access and Eligibility Services Program Policy
State Office 2106

Subject:
1. **SNAP Vehicle Asset Test**
2. **IRS FTI Security and Protection**
3. **Personal Needs Allowance Increase**
4. **Former Foster Care Children (FFCC) for Youth Who Aged Out of Foster Care in Another State**

The information in this bulletin will be included in a future handbook revision. Until the handbook is updated, staff must use the information in this bulletin. If you have any questions regarding the policy information in this bulletin, follow regional procedures.

Active bulletins are posted on the following websites:

- Medicaid for the Elderly and People with Disabilities Handbook (MEPDH) at https://hhs.texas.gov/laws-regulations/handbooks/mepd/policy-bulletins
- Texas Works Handbook (TWH) at https://hhs.texas.gov/laws-regulations/handbooks/texas-works-handbook/texas-works-bulletins.

1. SNAP Vehicle Asset Test

Background

House Bill (H.B.) 1287, passed by the 88th Texas Legislature, Regular Session, 2023, requires the Texas Health and Human Services Commission (HHSC) to increase the maximum excluded amount of a motor vehicle's fair market value (FMV) when determining eligibility for Supplemental Nutrition Assistance Program (SNAP).

Current Policy

SNAP

For all non-exempt vehicles, exclude up to $15,000 of the FMV for the highest valued vehicle and exclude up to $4,650 of the FMV for all other countable vehicles. The excess FMV is counted as a resource. (TWH A-1238, Vehicles)

New Policy

SNAP

For all non-exempt vehicles, exclude up to $22,500 of the FMV for the highest valued vehicle and exclude up to $8,700 of the FMV for all other countable vehicles. The excess FMV is counted as a resource.

Automation

Changes to TIERS are currently scheduled to be implemented with TIERS Release 116.1 on Dec. 23, 2023.

Correspondence

Correspondence changes are not required.

Handbook

Updates to the MEPDH are not required.

The TWH is currently scheduled to be updated in the April 2024 revision.

Training

Training is not required.

Effective Date

This policy is effective for all case actions disposed on or after Jan. 1, 2024.

2. IRS FTI Security and Protection

Background

The Internal Revenue Service (IRS) grants Texas Health and Human Services Commission (HHSC) permission to access Federal Tax Information (FTI) under the authority of Internal Revenue Code (IRC) 6103. HHSC uses this information to determine eligibility and accurate amounts of benefits for certain federally assisted benefit programs. As a condition of receiving access to FTI, HHSC agrees to establish and maintain safeguards to prevent the unauthorized access and disclosure of all tax returns and tax return information.

IRS completed a Safeguard Review in March 2023 and found that Texas HHSC does not have an adequate written policy and associated procedures for protecting media containing FTI. Although existing policies and procedures regarding IRS FTI Security and Protection are available for staff in the annual Safeguarding IRS Federal Tax Information Training, the purpose of this bulletin is to ensure existing policy regarding IRS FTI is clearly documented in the TWH and MEPDH.

Current Policy

All Programs

Current policy in the TWH and MEPDH only addresses general processes regarding the use of IRS FTI and instructs HHSC staff use the following forms to establish and maintain safeguards for IRS FTI:

- Form H1861, Federal Tax Information Record Keeping and Destruction Log;
- Form H1862, Federal Tax Information Transmittal Memorandum;
- Form H1863, Federal Tax Information Removal Log;
- Form H1864, Federal Tax Information Fax Transmittal; and
- Form H1866, Federal Tax Information Visitor Access Log. (TWH C-1050, Additional IRS FTI Sources and Security Issues, MEPDH C-2300, Custody of Records, MEPDH C-2400, Safeguarding Federal Income Data, MEPDH C-2500, Disposal of Records, and MEPDH C-2600, Procedure for Preventing Disclosures of Information)

New Policy

All Programs

The following existing policies and procedures regarding IRS FTI Security and Protection contained within the annual Safeguarding IRS Federal Tax Information Training are being added to the written handbook policy.

FTI includes tax returns or return information received directly from the IRS or obtained through an authorized secondary source, such as the Social Security Administration. Staff must protect digital and non-digital media containing FTI from unauthorized inspection and disclosure. Digital media includes computers, mobile devices, and removable items (e.g., CDs, DVDs, external hard drives, etc.). Non-digital media includes paper forms, reports, and logs.

HHSC limits FTI access to staff whose duties require access. HHSC agency and non-agency staff access FTI physically and through the Automated System for Office of Inspector General (ASOIG). Staff must handle FTI using the following policies to ensure the information does not become misplaced, stolen, or made available to unauthorized personnel.

FTI Security and Awareness Training

HHSC and non-HHSC staff who access or may potentially encounter FTI, must take and pass the annual Safeguarding IRS Federal Tax Information training to receive and maintain their access permissions to ASOIG. HHSC staff access the training course in System Training Solutions (STS) in the Centralized Accounting and Payroll/Personnel System (CAPPS). Non-HHSC staff may contact the HHSC IRS Coordinator via email at the HHSC AES Federal Tax Info Training Mailbox to obtain a copy of the training.

HHSC developed the *Safeguarding IRS Federal Tax Information Training* with role-based job aids as an agency resource for security and privacy awareness. HHSC updates this training on an annual basis to reflect any system and policy changes and address audit findings.

Upon completion of the *Safeguarding IRS Federal Tax Information Training*, HHSC staff submit a confirmation of understanding in STS. The confirmation acknowledges staff completed a thorough review of the web-based training and job aids in the resources tab relevant to their professional role. Additionally, it confirms understanding of incident reporting requirements. STS maintains a record of completion for each employee. Non-HHSC staff must review a PDF version of the training, sign Form H4096, Safeguarding Information Certification, and submit the form to their management. The form confirms completion and understanding of the material within the training, as well as the penalties involved for any unauthorized inspection and disclosure of FTI. Non-HHSC management must maintain a copy of the Form H4096 in the employee's file.

HHSC staff must also complete the *HHS Information Security/Cybersecurity Awareness Training* and the *HHS Privacy Training* within 30 days from their hire date and prior to accessing ASOIG. These trainings are available in STS in CAPPS.

Staff Access to FTI

HHSC and non-HHSC staff are prohibited from using personally owned media on agency systems or system components. Staff are also prohibited from using portable storage devices in agency systems when such devices have no identifiable owner.

HHSC and non-HHSC staff must adhere to policies and procedures related to the handling and protection of FTI to prevent unauthorized access and disclosure. Failure to adhere to the policies or procedures will result in disciplinary action, including warnings, access suspension, permanent access removal, or termination.

HHSC and non-HHSC management notify their staff within 72 hours when the formal employee sanction process is initiated. The notification includes the staff member sanctioned and the reason for the sanction.

HHSC and non-HHSC management must remove system and physical access when their staff transfer or are reassigned to a position that no longer requires ongoing operational need to access FTI. HHSC and non-HHSC management submit a modified access request within 24 hours of the transfer or reassignment.

HHSC and non-HHSC management must remove system and physical access and discuss information security during an exit interview when employment is terminated. HHSC and non-HHSC management submit a modified access request within 24 hours of the termination.

Physical Access to FTI

Work areas where staff physically access FTI should be limited to authorized personnel only. These areas must be prominently posted and separated from non-restricted areas by physical barriers that control access. FTI must be secured during and after normal operating hours. Staff accessing secured areas must clearly display a picture identification badge. The badge may not be obstructed and must be displayed above the waist.

Staff responsible for protecting access to FTI must mark system media, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. Additionally, staff responsible for protecting access to FTI must physically control and securely store media containing FTI within agency-controlled areas. Protect system media until it is sanitized or disposed of using approved equipment and methods.

Minimum Protection Standards

Minimum protection standards (MPS) require the agency to use at least two barriers to protect FTI from unauthorized access. These barriers include a combination of secured perimeters, security rooms, badged employees, and security containers.

- **Secured Perimeters** are enclosed by slab-to-slab walls constructed of durable materials and supplemented by periodic inspection. Any lesser-type partition must be supplemented by electronic intrusion detection and fire detection systems. All doors entering the space must be locked in accordance with Locking Systems for Secured Areas. In the case of a fence or gate, the fence must have intrusion detection devices or be continually guarded, and the gate must be either guarded or locked with intrusion alarms.
- **Security Rooms** are constructed to resist forced entry. The entire room must be enclosed by slab-to-slab walls constructed of approved materials (e.g., masonry brick or concrete) and supplemented by periodic inspection. Door hinge pins must be non-removable or installed on the inside of the room. Access must be limited to specifically authorized personnel.
- **Badged Employees** can serve as the second barrier during business hours between FTI and unauthorized persons. The authorized personnel must wear picture identification badges or credentials. The badge must be clearly displayed and worn above the waist.
- **Security Containers** are a storage device (e.g., turtle case, safe, vault, or locked IT cabinet) with a resistance to forced penetration, and a security lock with controlled access to keys or combinations.

Locking Mechanisms

All buildings, rooms, and containers containing FTI must be locked when not in actual use. Key or combination locking mechanisms may secure FTI. Staff not authorized to access FTI may have a key to the building but not the secured room. This includes unauthorized agency staff, contractors, security personnel, custodial staff, and landlords.

The following guidelines apply to key locking mechanisms:

- The number of keys must be kept to a minimum.
- Only authorized staff can access the secured area.
- The unauthorized duplication of keys is prohibited.
- Keys must be returned prior to departure for staff who retire, terminate employment, or transfer to another position.
- Management must conduct annual reconciliation of key records.

The following rules apply to combination locking mechanisms:

- The combination is only shared with authorized staff.
- The unauthorized disclosure of the combination is prohibited.
- Management must change the combination at least once annually or upon departure of staff that retire, terminate employment, or transfer to another position.

Authorized Access, Visitor Access, and Authorized Personnel Lists

HHSC must maintain a visitor log and authorized access list (AAL) to record access to physical work areas containing FTI. Staff maintain Form H1866 as a record of visitor access to a restricted area. Security staff must validate a visitor's identity by examining a government-issued identification (state issued identification, driver's license, or passport). An AAL is maintained and MPS enforced to facilitate the entry of staff who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area. The AAL must contain the following:

- name of employee, vendor, contractor, or non-agency personnel;
- name of agency or department;
- name and phone number of the agency point-of-contact authorizing access;
- address of agency, vendor, or contractor; and
- purpose and level of access.

HHSC management must review the AAL monthly or upon potential indication of an event such as a security breach or personnel change. HHSC management must maintain an authorized personnel list of all staff who have access to information systems areas containing FTI.

Access Control Systems

Access control systems (e.g., badge readers, smart cards, or biometrics) that provide the capability to audit access control attempts must maintain access control logs with successful and failed access attempts to secured areas containing FTI or systems that process FTI. Management must review access control logs monthly. Access control logs must contain the following information for each access request:

- the name of the access control device owner;
- the successful or failure result of the access request; and
- the date and time of the access request.

FTI Transport

Staff must transport media containing FTI in a way that prevents loss or unauthorized disclosure. The IRS prohibits staff from transmitting FTI via agency email systems, Microsoft Teams, or by phone. Staff must not use HHSC email

addresses to send confidential or agency-sensitive information to personal email addresses.

Staff must secure computers and electronic media that receive, process, store, access, protect, or transmit FTI in an area with restricted access. The agency must use encryption mechanisms on all computers and mobile devices that contain FTI to prevent access if lost or stolen. Staff must label removable media containing FTI.

Authorized staff must keep all computers, electronic media, and removable media containing FTI in their immediate protection and control during use. When not in use, authorized staff must secure the device in the proper storage area or container. Staff may not leave devices unattended in a public area. HHSC management must maintain inventory records of computers, electronic and removable media, and complete a semi-annual review for control and accountability.

In-Person Transport

Staff transporting media containing FTI must always keep it in their possession. Never leave FTI unattended in a public setting. Use Form H1863 when removing FTI from a file and retain the form for five years from the last FTI removal indicated.

For office relocations, ensure plans include the proper protection and accountability of all FTI. Staff must lock FTI in cabinets or sealed packing cartons while in transit. HHSC staff maintain custody of FTI to ensure cabinets or cartons containing FTI are not misplaced or lost in transit.

Mail or Courier Transport

Double seal all FTI transported through the mail by sealing one envelope within another envelope. On the inner envelope, staff must mark "Confidential" with some indication that only the designated recipient is authorized to open it. Do not label the outermost envelope as FTI or provide any indication that it contains FTI. Use Form H1862 when mailing all paper documents that contain IRS data. The sender ensures the receiver acknowledges the receipt of the information.

Fax Transport

Fax machines must be placed in a secure area and staff should refrain from faxing FTI, when possible. There must be trusted staff at both the sending and receiving fax machines. When faxing is required, staff must use Form H1864. The form must accompany all faxed documents that contain IRS data when transferred from one office to another or from an office to a banking institution for verification purposes. The sender ensures the receiver acknowledges the receipt of the information and retains this form for five years.

FTI Sanitation

The sanitization process removes FTI from media to ensure the information cannot be retrieved or reconstructed. Examples include but are not limited to digital media found in scanners, copiers, printers, computers, network components, mobile devices, and non-digital media such as paper and microfilm. Staff must use agency-approved software and methods for sanitizing FTI. The following are acceptable sanitization methods:

- **Clearing** protects the confidentiality of information against a robust keyboard attack. Simple deletion of items is not sufficient. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts. Overwriting is an example of an acceptable clearing method.
- **Purging** protects the confidentiality of information against a laboratory attack. This type of attack involves using signal processing equipment and specially trained personnel. Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable purging methods.

HHSC must maintain sanitization records which include the:

- control number, file name and contents, or both for each record;
- total number of records;
- date and method of sanitation; and
- date of sanitization verification.

FTI Destruction

The destruction process ensures that media with FTI cannot be reused as originally intended. Examples include but are not limited to disintegration, incineration, pulverizing, shredding, and melting. Staff use Form H1861 to record and track the destruction of FTI. If non-HHSC staff destroy FTI, an HHSC employee must witness the destruction. Staff must use HHSC approved methods for destroying FTI.

The following are acceptable destruction methods:

- **Incineration** ensures the incinerator is certified and produces enough heat to burn the entire bundle. If it cannot burn the entire bundle, separate the pages to ensure all materials are incinerated.
- **Shredding** ensures a crosscut shredder which produces particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller) is used. If shredding deviates from these specifications, then the FTI must be safeguarded until it

reaches the stage where it is rendered unreadable through additional means, such as burning or pulping.
- **Disintegration or Pulverization** ensures a device is equipped with a 3/32 in. (2.4 mm) security screen.

HHSC must maintain destruction records which include the:

- date the records were received;
- control number, file name and contents, or both for each record;
- name of the person receiving the records;
- total number of records, if available;
- movement of records from receipt to destruction; and
- date and method of destruction.

Reporting FTI Security Incidents

FTI security incidents include loss of control, unauthorized access, unauthorized disclosure, or unauthorized inspection. Upon discovering an actual or possible compromise of IRS FTI or an unauthorized inspection or disclosure of IRS FTI, including breaches and security incidents, the person observing or receiving the information must immediately contact the HHSC IRS Coordinator within 24 hours of initial discovery. Send a secure email with the subject line, *URGENT: FTI Data Incident Report* to the HHSC IRS Coordinator Mailbox.

The HHSC IRS Coordinator reports the incident by:

- contacting the office of the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA); and
- following the IRS Office of Safeguards, as directed in Section 10.2 of IRS Publication 1075.

In the event the HHSC IRS coordinator fails to respond by the close of the next business day, staff immediately inform management by sending an email with the subject line, *URGENT – POSSIBLE UNAUTHORIZED DISCLOSURE OR INSPECTION OF FTI* to HHSC Offices for Information Technology, Privacy Division, Chief Information Security Office, and IRS coordinator.

Examples of FTI security incidents include but are not limited to:

- leaving an agency computer or laptop with FTI unlocked and unattended;
- leaving a file cabinet with FTI unlocked;
- allowing contract IT Help Desk support access to an agency device with FTI while the user is accessing ASOIG;
- printing FTI on Xerox Multi-Factor Office Devices;

- allowing unmonitored contractor access to an FTI hardware server;
- discussing FTI on a Voice over Internet Protocol (VoIP) phone with people or other agency employees;
- viewing FTI remotely without approval;
- sending screenshots of FTI data from the ASOIG application;
- screensharing FTI during virtual meetings, including meetings conducted through Microsoft Teams, Zoom, Go To Meeting, Webex, Google Meet, etc; and
- stealing or losing laptop computers, removable devices, or non-digital media containing FTI.

Penalties for Disclosing FTI

People responsible for the willful unauthorized inspection or disclosure of FTI may be subject to criminal and civil penalties, in addition to disciplinary action. Security incidents may also result in temporary or permanent suspension from ASOIG access.

Criminal penalties for willful unauthorized inspection of FTI are:

- a fine up to $1,000; and
- one year in prison, together with the costs of prosecution.

Criminal penalties for willful unauthorized disclosure of FTI are:

- a fine up to $5,000; and
- up to five years in prison, together with the costs of prosecution.

Civil penalties for willful unauthorized inspection or disclosure of FTI are:

- the greater of $1,000 or actual damages for each incident; and
- court costs and attorney fees to the plaintiff.

Automation

Automation changes are not required.

Correspondence

Correspondence changes are not required.

Handbook

The MEPDH is currently scheduled to be updated in the June 2024 revision.

The TWH is currently scheduled to be updated in the July 2024 revision.

Training
Training is not required.

Effective Date
This policy is effective Dec. 11, 2023.

3. Personal Needs Allowance Increase

Background

When determining the co-payment for a person receiving services in an institutional setting, HHSC deducts a personal needs allowance (PNA). The PNA is the amount of income the Medicaid recipient may retain for their personal use. For Supplemental Security Income (SSI) recipients who reside in an institutional setting and are eligible for a reduced federal payment of $30 from the Social Security Administration, HHSC provides a state supplement payment to ensure the recipient has access to the minimum PNA established by the legislature.

House Bill (H.B.) 54, passed by the 88th Texas Legislature, increases the minimum PNA for Medicaid recipients residing in a nursing facility (NF) or an intermediate care facility for persons with an intellectual disability or related conditions (ICF/IID).

Current Policy

MEPD

When determining the co-payment for a person receiving services in an institutional setting, the PNA is $60 per month for an individual and $120 per month for a couple. (MEPDH H-1500, Personal Needs Allowance, and MEPDH H-4100, Individual and Couple Cases)

SSI recipients who reside in an institutional setting and only receive the $30 reduced federal benefit payment, receive a $30 supplement payment from the state. (MEPDH H-1500, Personal Needs Allowance)

New Policy

MEPD

Effective Jan. 1, 2024, the monthly PNA increases to $75 per month for an individual and $150 per month for a couple.

SSI recipients who reside in an institutional setting will receive a $45 state supplement payment.

Note: SSI recipients will receive January 2024 state supplement payment in February 2024.

Automation

Changes to TIERS are currently scheduled to be implemented with TIERS Release 116.1 on Dec. 23, 2023.

Correspondence
Language will be added to the TF0001, Notice of Case Action, to inform recipients of the change in co-payment due to the increase in the PNA.

Handbook
The MEPDH is currently scheduled to be updated in the March 2024 revision.

Updates to the TWH are not required.

Training
Training is not required.

Effective Date
This policy is effective Jan. 1, 2024.

4. Former Foster Care Children (FFCC) for Youth Who Aged Out of Foster Care in Another State

Background

On Oct. 24, 2018, the Substance Use-Disorder Prevention that Promotes Opioid Recovery and Treatment (SUPPORT) for Patients and Communities Act, was enacted. Section 1002(a) of the SUPPORT Act requires states to extend Medicaid eligibility to youth who transitioned out of foster care in a different state and were receiving federally funded Medicaid when they aged out. This change is effective for youth who turned age 18 on or after Jan. 1, 2023.

Current Policy

FFCC

To be eligible for FFCC, a person must be aged 18 to 26 and:

- aged out of foster care in the state of Texas at age 18 or older;
- received federally funded Medicaid when they aged out of foster care; and
- meet all other Medicaid eligibility criteria, including Texas Residency and U.S. citizenship or alien status.

(TWH E—111, Type of Assistance (TA) 82 – Medical Assistance – FFCC)

New Policy

FFCC

To be eligible for FFCC, a person must be aged 18 to 26 and:

- aged out of foster care in any state at age 18 or older;
  - **Note:** Individuals who turned 18 prior to Jan. 1, 2023, must have aged out of foster care in the state of Texas.
- received federally funded Medicaid when they aged out of foster care; and
- meet all other Medicaid eligibility criteria, including Texas residency and U.S. citizenship or alien status.

Staff Procedures

Staff must follow the applicable policy when processing applications for FFCC:

- If the person turned age 18 prior to Jan. 1, 2023, and aged out of foster care at age 18 or older **in Texas**, determine eligibility according to **Current Policy**.
- If the person turned age 18 on or after Jan. 1, 2023, and aged out of foster care at age 18 or older **in any state**, determine eligibility according to **New Policy**.

If the person aged out of foster care in another state, verify the person's former foster care status and Medicaid enrollment status from the other state. Acceptable verification sources include:

- official form, notice, or statement from the out-of-state foster care agency;
- court order; or
- contact with out-of-state agency.
    - A mandatory text box in the Texas Integrated Eligibility Redesign System (TIERS) **Individual – Individual Information** logical unit of work (LUW) requires staff to document the details about out-of-state agency contact including the person's name, phone number, and other relevant information.

Follow the steps below to locate the out-of-state agency contact information and make collateral call(s) to verify former foster care and Medicaid enrollment statuses for youth who aged out of foster care on or after Jan. 1, 2023.

1. Enter the following link in a web browser: https://www.medicaid.gov/about-us/contact-us/index.html.
2. Select the appropriate state from the "Contact Your State Medicaid Agency" drop-down and then select "go".
3. Identify the best contact number and attempt to make collateral call(s) to obtain the verification. If collateral call is:
    a. Successful, answer the former foster care related questions in the **Individual – Individual Information** LUW in TIERS, select "contacted out of state agency" as the verification source in the new "Verification of Medicaid Enrollment" drop down, and document the state agency contact person's name, phone number and any additional information in the mandatory text box field.
    b. Unsuccessful, answer the former foster care related questions in the **Individual – Individual Information** LUW in TIERS, select "Not Verified" in the new "Verification of Medicaid Enrollment" drop down, and send Form H1020, Request for Information or Action.
4. Document any failed collateral call attempts in Case Comments.

Staff must follow the current policy when an applicant recently received benefits in another state, including verifying the last month the benefits were issued. (TWH A—720, New Texas Residents; A—822, Medicaid Coverage for New State Residents)

Automation
Until TIERS automation changes are completed, staff are instructed to follow Continency Processing Method (CPM) #1162893, Former Foster Care Children (FFCC) for Youth Who Aged Out of Foster Care in Another State, to provide FFCC Medicaid to eligible youth.

Changes to TIERS are currently scheduled to be implemented with TIERS Release 116.1 on Dec. 23, 2023.

Correspondence
The former foster care related questions on Form H1265, Presumptive Eligibility Worksheet, will be updated according to new policy and federal requirements.

Handbook
Updates to the MEPDH are not required.

The TWH is currently scheduled to be updated in the April 2024 revision.

Training
Training will be available in the Program Area Learning Management System (PALMS) as part of R116.1 General Information on Dec. 15, 2023.

Effective Date
This policy is effective with the release of this bulletin and must be retroactively applied for any case actions on or after Jan. 1, 2023.