

TEXAS WORKFORCE COMMISSION LETTER

ID/No: WD 01-04

Date: January 26, 2004

Key Words: TANF/Choices /
FSE&T / Child Care

To: Local Workforce Development Board Executive Directors
Commission Executive Staff
Integrated Service Area Managers
Commission Local Offices

From: Luis M. Macias, Director, Workforce Development Division

Subject: Accessing Information in the Texas Health and Human Services
Commission's Texas Integrated Eligibility Redesign System

PURPOSE:

To provide Local Workforce Development Boards (Boards) with information on accessing benefit data for current or former recipients in the new Texas Health and Human Services Commission (HHSC) (formerly Texas Department of Human Services) automated system—the Texas Integrated Eligibility Redesign System (TIERS).

REFERENCE:

Texas Integrated Eligibility Redesign System Inquiry for Workforce Network Reference Guide, issued June 2003

FLEXIBILITY RATINGS:

No Local Flexibility (NLF): This rating indicates that Boards must comply with the federal and State laws, rules, policies, and required procedures set forth in this WD Letter and have no local flexibility in determining whether and/or how to comply. Federal and State laws, rules, policies, and required procedures with a “No Local Flexibility” rating are indicated by the acronym, **NLF**, in the margin to the right of the applicable paragraph. Additionally, all information with a “No Local Flexibility” rating is indicated by “must” or “shall.”

Failure to comply with the federal and State laws, rules, policies, and required procedures with a “No Local Flexibility” rating may result in corrective action, up to and including sanction and penalty.

Local Flexibility (LF): This rating indicates that Boards have local flexibility in determining whether and/or how to implement guidance or recommended practices set forth in this WD Letter. All guidance or recommended practices with a “Local Flexibility” rating are indicated by the acronym, **LF**, located in the margin to the right of the applicable paragraph. Additionally, guidance or recommended practices with a “Local Flexibility” rating are indicated by “may” or “recommend.”

Boards are not subject to corrective action for failure to comply with guidance or recommended practices with a “Local Flexibility” rating.

BACKGROUND:

HHSC has developed a new automated system, TIERS, which is being piloted in two local workforce development areas (workforce areas). Upon successful completion of the pilot programs, TIERS will replace the System for Application, Verification, Eligibility, Referral, and Reporting (SAVERR) and will be available to all workforce areas.

Two Boards—Capital Area and Rural Capital Area—are piloting TIERS in five Texas Workforce Centers. All Temporary Assistance for Needy Families (TANF) and Food Stamp Employment and Training (FSE&T) recipients in those two workforce areas are included in the TIERS pilot.

Therefore, **effective immediately**, benefit information on recipients in these workforce areas is accessible only through TIERS, and is no longer available in SAVERE—even if a recipient moves to a workforce area that is not included in the pilot program.

The implementation of TIERS affects only how benefit information is accessed; it does not affect existing service delivery requirements for TANF/Choices, FSE&T, or child care services.

PROCEDURES:

Boards must ensure that all appropriate staff—including workforce partners, such as child care providers and one-stop operators—have access to TIERS.

NLF

How to Obtain Access to TIERS

The Workforce Information System of Texas (TWIST) administrators must complete the forms included as Attachments 1 and 2 to this WD Letter. Instructions on completing and submitting the forms are included in Attachment 3 to this WD Letter.

NLF

Designated Access to TIERS

It is recommended that Boards:

LF

- designate at least one person at each Texas Workforce Center to have TIERS Inquiry access; and
- request TIERS Inquiry access as soon as possible because it takes approximately two weeks to secure access once the request is forwarded to HHSC.

Boards must process clients in TIERS in the same manner they are processed in SAVERR. This includes information on:

- Choices and FSE&T Good Cause;
- Choices and FSE&T Penalty Requests; and
- Choices Demonstrated Cooperation.

The current version of the TIERS Inquiry for Workforce Network Reference Guide (guide), issued in June 2003, can be accessed on the Texas Workforce Commission (Commission) **Intranet** on the **Training & Development** homepage, listed under **Resources/Desk Aids** at:

<http://intra.twc.state.tx.us/intranet/train/html/index.html>. The guide will be maintained and updated as needed.

Instructions on accessing TIERS for external Commission partners are available at: http://rsaus60.dhs.state.tx.us/im/docs/ExtAgcy/TIERS_External_Access.htm.

For more information on TIERS, consult the Health and Human Services Consolidated Help Desk at (512) 438-4720.

ACTIONS REQUIRED:

Boards must ensure that appropriate staff are apprised of and comply with the requirements in this WD Letter.

INQUIRIES:

Direct inquiries regarding this WD Letter to your workforce area’s assigned contract manager.

ATTACHMENTS:

- Attachment 1: Computer Security Agreement (Form 4014)
- Attachment 2: Request for Applications & System Access (Form 4743)
- Attachment 3: Instructions for Completing Forms 4743 and 4014

Rescissions: None	Expiration: Continuing
-------------------	------------------------

COMPUTER SECURITY AGREEMENT

Name	Social Security No.	Div./Reg. (1 st 3 digits of BJN)	Unit (4 th and 5 th digits of BJN)	Mail Code
Provider Agency Name		Business Telephone No. (inc. area code) () - -		

The following policies and procedures exist to provide data security, protect privacy, and ensure confidentiality and integrity to client, employee, and administrative information accessed via automated systems within the Texas Department of Human Services (DHS). Please read the following agreements carefully and thoroughly before signing. You must sign and date all four agreements on pages 1, 2, and 3.

I understand that in performance of my assigned job duties during my employment with DHS, I may receive identification codes (ID) and/or passwords (also known as security codes) for the DHS computer network. I understand that any issued ID and/or password are for official state-approved business only. I understand that the IDs and/or passwords are to be used only by me, and that I am not to disclose any security codes to anyone or allow anyone to use my IDs and/or passwords. I understand that I am responsible for any actions done under my ID. I agree to change all passwords immediately whenever the need exists, for example, if someone learns my password or the password becomes known during problem resolution or day-to-day functions.

I understand that I am prohibited from changing any software (including, but not limited to, display screens, operating system instructions, and applications) that reside on any DHS system or automated storage medium unless this change is approved by an authorized person.

I understand that I am prohibited from accessing any automated system, subsystem or automated storage medium for which I have not previously received proper authorization. I further understand that I am prohibited from altering any data or database other than that which is specifically authorized as required in the performance of my job functions.

I understand that if I have any questions or problems, I am to immediately report the situation to my supervisor or automation support staff.

I agree to follow policies and procedures related to data security and data confidentiality in handbooks and manuals issued by DHS automation authorities and any additions, deletions, or revisions thereto.

I have read Form 4014, Pages 1 and 4, related to data security and data confidentiality. I understand that these and the above stated policies and procedures apply to all security codes I receive to conduct state-related business. I understand that failure to follow the policies, procedures, and laws of the State of Texas may result in loss of access to the computer system(s) and/or disciplinary action, which may include dismissal and criminal prosecution.

Signature

Date

Computer Security Agreement

As an authorized user of the Internal Revenue Service (IRS) Match Inquiry System, I understand the information obtained from the system may be used for official state-approved business. I understand my user ID and password is to be used only by me. Under no circumstances will I reveal or allow use of my password by another person.

I understand printed IRS inquiries must be stored in a locked container or room and printed IRS data must be destroyed according to confidential trash procedures established by DHS.

I understand if I fail to follow any of these standards, I may be subject to disciplinary action and/or prosecution. Unauthorized disclosure of IRS data can result in a felony conviction punishable by a fine up to \$5,000 and/or up to five years in prison.

I understand and agree to follow the security procedures stated in this agreement.

Signature

Date

Program Area Approval for Non-State Staff _____

Data Broker

As an authorized user of the Data Broker system, I understand the information obtained from the system may be used for official state-approved business. I understand my user ID and password is to be used only by me. Under no circumstances will I reveal or allow use of my password by another person.

I understand that inappropriate use of Data Broker information is a work rule violation and will result in disciplinary action up to and including dismissal.

I agree to request Data Broker credit reports only when permissible purpose exists. I understand that "permissible purpose" means that the individual whose credit report I request must be:

- An applicant or recipient of TANF or Food Stamps, or
- A household member who would be included in the TANF or Food Stamp case except that he is disqualified or ineligible.

I have been informed that requesting a credit report without permissible purpose is a violation of federal law and may result in civil liability.

I understand that requesting a Data Broker credit report for purposes not associated with determining eligibility for Texas Works programs is a work rule violation and will result in a recommendation for dismissal.

I understand and agree to follow the security procedures stated in this agreement.

Signature

Date

Computer Security Agreement

Wired Third Party Query System

I acknowledge that, as a receiving agency user, I have been assigned a personal user identification code (User ID) and password which I will use to activate the Wire Third Party Query (WTPY) system that allows access to information provided by the Social Security Administration. I understand that I will be held personally accountable for my actions and any activity performed under my password. Under no circumstances will I allow my user ID and confidential password to be used by any other individual, nor will I use one belonging to someone else. I will not enter any unauthorized data, make any unauthorized changes to data or disclose any information without prior authorization. Violating a data security system or allowing unauthorized access by another party, is a class A misdemeanor under Chapter 33 of the Texas Penal Code and punishable by a fine of \$3,000, a year in Jail, or both. Intentionally causing a computer to malfunction or knowingly altering data without authorization, that results in personal or property damage, may constitute a felony of the second degree.

I agree to abide by the Social Security Administration Wire Third Party Query System information security operating procedures and standards. I also understand that if I violate any of these standards I may be subject to disciplinary action or prosecution under one of more applicable statutes, and I may jeopardize the agreement between the Texas Department of Human Services and the Social Security Administration.

Signature of User

Date

Computer Security Agreement

It should be emphasized that all DHS employees have a responsibility for contributing to the security of equipment and information. Certain individuals may have primary responsibility, but all employees have a part in protecting equipment and data. (*Automation and Telecommunications Handbook (ATH)* [3000])

All automated equipment operators have the responsibility to ask for names and purposes of visits from people who do not seem to be known by any staff in the area of the equipment. (3000)

Whenever possible, screens of terminals should be placed so visitors or passersby cannot see confidential information on the screen. This may not be practical for single-user microcomputers. The back of a microcomputer should not be turned to the outside of the desk, as accidental powering off could occur. (3000)

Do not use employee initials or something easily guessed for a password. The importance of keeping passwords confidential must be emphasized to staff. (3000)

Destroy all printouts and carbons from printouts according to procedures in item 7240, Destruction of Records, in the *Administrative Management Handbook (AMH)*. (3000)

Do not remove equipment from the premises without signing out the equipment with the data communications manager, office manager, or division administrator, or regional director for Texas Works or Long Term Care Services.

Any employee sharing his access is subject to appropriate disciplinary action. (3000)

DHS policy regarding sharing use of state computer systems is included in the *ATH*, Item 3520, Use of Hardware and Software. This policy covers usage of DHS hardware and software.

Data Integrity and Security

All use of agency owned or leased computer systems must be for officially authorized purposes only. The use of DHS computer systems for non-agency consulting work or unofficial purposes without the written approval of the commissioner is prohibited. The sale of DHS computer system time outside DHS requires the prior written approval of the commissioner.

All computer programs and data are for the sole use of DHS. All computer programs and data developed for DHS by consultants or vendors are the property of DHS and must be returned to DHS upon project completion or termination, unless a written release is granted by the commissioner.

The commissioner or his designee is responsible for the proper authorization of computer utilization by the agency and the establishment of effective use.

MIS is responsible for the security and integrity of data in category 1 and 3 systems. For category 2 systems, the approving authority for a system or database is responsible for the integrity of data and its external and internal security.

Copies of any programs or data may only be released for DHS computer systems upon written authorization of the commissioner or his designee.

Before the last day of employment, an employee who leaves DHS must return to the supervisor all department property and equipment used in connection with computer systems.

Questions concerning the appropriateness of the release of a data file or computer program should be directed to the employee's supervisor or the appropriate regional administrator, assistant commissioner, or above.

Copyright laws have been made to protect the rights of both the users and the creators of documents and other original material. All users have the responsibility for avoiding copyright violations during use of automation technologies. This includes both copying and altering licensed software and applies to systems software, application packages, documentation, or other material provided by vendors. The regional administrator is responsible for safeguarding the copyrights of vendor-supplied software. System software must not be used on non-DHS equipment. (ATH 3000)

Because client information is confidential, precautions must be taken to limit unauthorized access to client information. Requesters should submit requests for inquiries and disclosure of information. (AMH 8100)

By law, information in DHS files is confidential. Only authorized staff may change confidential information. It is unlawful to change, alter, or damage files without expressed permission. (TX Criminal Law, PC 33.03)

In addition to restricting unauthorized access to information on computer files, the operator must be aware of the limitations on releasing information on computer files. Additional restrictions are placed on requests from non-DHS users. If there is a question about the release of information, contact the supervisor.

Employees are expected to not willfully or negligently damage, misuse, lose, or sell state property, department equipment, or materials for personal use or monetary gain. (*Human Resource Services Handbook*, Item 4700, Agency Rules and Requirements.)

Provider Agency Requirements

By law, information in DHS files is confidential, except for purposes directly connected with the administration of an assistance program. It is a criminal offense to release information from DHS files. The maximum punishment is one year in jail and/or \$3000 fine. (*Human Resources Code*, Sec. 12.003)

The provider agency is responsible for notifying DHS of the termination of employment of any staff who has signed a computer security agreement.

Computer Security Agreement

Users seeking access to IRS provided data, complete the top information portion of the Computer Security Agreement on page 1 of this form. It is optional if you want to complete the provider agency name section. Read the last four paragraphs on page 1, then sign and date the statements at the bottom of the page.

The four excerpts (exhibits 1-4 below) summarize the larger briefing material that is maintained with other policies and procedures within your unit.

Exhibit 1

Returns and return information shall be confidential.

During employment, as well as after a person terminates employment, laws preclude that person from disclosing tax return information.

Return information includes many pieces of information and is not limited to the taxpayer's name, source and amount of income, payments, deductions and net worth.

This section also includes definitions of terms.

Exhibit 2

This section deals with safeguarding information. Ensure you apply rules approved by your management.

Follow the rules on destruction and storage of Federal Tax Information (FTI). (Only share information with an approved office or individual that is authorized to use FTI in the performance of their duties.)

Exhibit 3

Exhibit three spells out the penalties for disclosing tax information.

Any violation is a felony and if convicted, one can receive a fine up to \$5,000 or be imprisoned for not more than 5 years.

It is also a felony to unlawfully receive FTI and disclose that information in a manner not approved by this title.

Exhibit 4

Exhibit four outlines the civil damages a person or an agency can incur for disclosing FTI.

No liability will occur if the disclosure is in good faith or at the request of the taxpayer.

Damages can be assessed at \$1,000 per disclosure or the sum of the actual damages.

A plaintiff can file a complaint up to two years from time of discovery.

REQUEST FOR APPLICATIONS & SYSTEM ACCESS

**FAX TO: Management Information Services
State Office C-732, FAX (512) 438-5288**

FROM: TEXAS WORKFORCE COMMISSION

FOR SECURITY	Password	Password	Password	Password	Password
System Designator	City	Region	Mail Code	Type of USER Change <input type="checkbox"/> Add New <input type="checkbox"/> Delete <input type="checkbox"/> Modify	
Employee Name (last, first, MI) Name as appears in AASS			Effective/Hire/Termination Date	BJN	
Employee No.	Social Security No.		Employee Phone No. (inc. area code & extension)		
E-Mail		Employee Title / Contractor			
IRIS: <input type="checkbox"/> Production <input type="checkbox"/> Development <input type="checkbox"/> Mapper Dept./Cabinet: _____					

TEXAS DEPARTMENT OF HUMAN SERVICES:

1. Non-LAN Financial Servs Limited Inq Full Inq 2. Non-LAN Financial Servs Data Entry 3. FMIS Inq DE 4. HRMIS SO REG Inq DE 5. Medical Provider Services Inquiry 6. LAN LSC 7. TAMENU	8. Texas Works Clerk Worker 9. LTCS Clerk Worker 10. BCMASST Inq DE 11. TWC 12. OAG 13. Broadcast Texas Works LTCS X 14. Other TIERS - TWC
---	---

CLIENT SERVER / RMO APPLICATIONS:

1. OUTLOOK 2. DATA BROKER 3. WTPY 4. IRS 5. DIAL-UP 6. ARTS WEB 7. MDS	8. OPI 9. CASE TRACKING APP for OGC 10. CARES 11. ALZHEIMERS 12. TEXAS WORKS REDIRECTS 13. TEXAS WORKS SCHEDULER 14. ASPEN	15. CMS SASO PROVIDER 16. CCAD CASELOAD REALIGNMENT 17. IWS / INCOME & ELIGIBILITY VERIFICATION 18. PMRS 19. PMRS PROJECT MANAGER/LIBRARIAN 20. RMO Applications: _____ 21. Other _____
--	--	---

CLIENT SERVER DATABASE: Server: _____ Add Delete Modify **DBA Use Only**

Database/Schema	Group/Alias/Role	Effective Begin Date	Effective End Date	Action Taken

DBA USE ONLY:
 Login: _____ Completed By: _____ Date User Notified: _____
 Password: _____ Completed Date: _____

UNIX: User Administrator **Required Access Dates**

System: _____ Request Group: _____ Start: _____
 Alternate Directory: _____ Preferred Shell: _____ End: _____

_____ **Print Name - Supervisor** _____ **Signature - Supervisor** _____ **Date** _____ **Phone #**

Signature - Regional Automation Director _____ **Date** Comments: _____

FOR SECURITY SECTION USE ONLY

Approved **Disapproved** Reg. Comments: _____
 MIS Comments: _____

Signature - Security _____ Date _____ PAC: _____
 RD/RMO: _____

Instructions for Completing Forms 4743 and 4014

For Users Requesting TIERS Access:

A. Form 4743 requires the FROM field at the top of the form to display the Agency/Division/Group or Section of the requestor. Enter **TEXAS WORKFORCE COMMISSION**.

- In the City field, enter the city associated with the employee. If it is known, enter the two-digit region code in the appropriate field. If you do not know the region code, contact Mary Blake at mary.blake@twc.state.tx.us.
- Mark an “X” in the box next to Add New.
- The user enters his or her name as LAST, FIRST, MI in the Employee Name field.
- Though not required, the Social Security number (that is still used on some systems) aids in the processing of the request.
- Enter the user’s phone number including area code and extension.
- If the user has an e-mail account, enter it in the appropriate field.
- Enter the user’s job title and/or functional position.
- On line #14, check Other and next to Other, enter “TIERS - TWC” if it has not already been added.
- Near the bottom of the form, fill in the Supervisor fields with an appropriate authorized name. This person will then sign and date the appropriate fields, and provide a phone number including area code and extension. The person signing the Supervisor field will be responsible for ensuring that the person named on Form 4743 is authorized for the requested access.
- Only authorized TWC Security employees should sign the Regional Automation Director field. E-mail completed forms to Mary Blake at mary.blake@twc.state.tx.us or Kathy Kelsey at kathy.kelsey@twc.state.tx.us for signature.

B. Form 4014 is to accompany Form 4743 for any user requesting access to TIERS.

- On Form 4014, enter the user’s name in the appropriate field as LAST, FIRST, MI.
- Enter the user’s Social Security number. (Disregard the boxes associated with BJN and Mail code.)
- In the Provider Agency Name box, enter “Texas Workforce Commission.”
- Enter the user’s phone number including area code and extension.
- Have the user sign and date at the bottom of the form.