TEXAS WORKFORCE COMMISSION LETTER

ID/No:	WD 02-18
Date:	March 23, 2018
Keyword:	Administration; All Programs; General
Effective:	Immediately

To: Local Workforce Development Board Executive Directors
Commission Executive Offices
Integrated Service Area Managers
Texas Workforce Commission Agency Grantees

From: Courtney Arbour, Director, Workforce Development Division

Subject: **Handling and Protection of Personally Identifiable Information and Other Sensitive Information**

PURPOSE:

To provide Local Workforce Development Boards (Boards) and Texas Workforce Commission (TWC) Grantees (grantees)[1] with information and guidance on handling personally identifiable information (PII) and other sensitive information, specifically:

- requirements for the handling and protection of PII; and
- recommended best practices.

RESCISSION:

WD 13-13

BACKGROUND:

The US Department of Labor Employment and Training Administration (DOLETA) Training and Employment Guidance Letter 39-11, issued June 28, 2012, and entitled "Guidance on the Handling and Protection of Personally Identifiable Information (PII)," requires that strong and effective measures be taken to mitigate the risks associated with the collection, storage, dissemination, and disposal of sensitive data, including PII.

Based on the Office of Management and Budget (OMB) and DOLETA definitions, TWC defines PII and other sensitive information as follows:

- PII—information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII includes, but is not limited to, Social Security numbers (SSNs), credit card numbers, bank account numbers, home

[1] TWC's Integrity of the Texas Workforce System rule §802.2(1) defines Agency Grantees as "grantees that receive funding from the Agency, such as Skills Development Fund, Wagner-Peyser 7(b), and Workforce Investment Act (WIA) statewide, to provide workforce services."

telephone numbers, mobile telephone numbers, ages, birth dates, marital status, spouse names, educational history, biometric identifiers (for example, fingerprints, voiceprints, and iris scans), medical history, financial information, and computer passwords

- Other sensitive information—any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of federally funded programs, or the privacy to which individuals are entitled under the Privacy Act of 1974, as amended (5 USC §55a)

As part of their grant-funded activities, Boards and grantees have in their possession large quantities of PII and other sensitive information relating to their organizations and staffs, subcontractor and partner organizations and staffs, and individual program participants. This information is generally found in personnel files, participant data, performance reports, program evaluations, grant and contract files, and other sources.

Protection of PII can be provided for documents or systems in several ways. How the required protection is provided depends on the facility, the function of the activity, how the activity is organized, and what equipment is available. Proper planning and organization will enhance the protection of PII while balancing the costs.

Minimum protection standards (MPS) establish a uniform method and minimum standards of physically protecting data and systems that require safeguarding. These standards must be applied. Because local factors might require additional security measures, management must analyze local circumstances to determine space, container, and other physical security needs.

MPS require two barriers for the protection of PII under normal operating conditions. Some examples of barriers are:

- Staff presence
- Locked office, locked file cabinet, or another lockable container
- Access control system such as a card reader
- Restricted access by means of keypad entry or secondary-level card key access
- Out of plain sight; as a second barrier only

The following table contains examples of combining two barriers to protect PII at locations used by the Board and contractors and by grantees (for example, Board offices, Workforce Solutions Offices, and other affiliated sites):

Area	PII Barrier 1		PII Barrier 2
	During Hours of Operation	After hours	
Restricted*	Staff serves as an escort to all visitors and monitors visitor activity	Locked building, security guard	Out of plain sight

Area	PII Barrier 1		PII Barrier 2
	During Hours of Operation	After hours	
Secured	Authorized staff only	Locked building, security guard	Locked; access control
Public	Staff monitored	Locked building, security guard	Locked; staff distributes documents with PII to customers

*****As identified by signage such as "Employees Only"

PROCEDURES:

No Local Flexibility (NLF): This rating indicates that Boards and grantees 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. All information with an NLF rating is indicated by "must" or "shall."

Local Flexibility (LF): This rating indicates that Boards and grantees have local flexibility in determining whether and/or how to implement guidance or recommended practices set forth in this WD Letter. All information with an LF rating is indicated by "may" or "recommend."

Handling and Protection of Personally Identifiable Information and Other Sensitive Information

NLF: Boards and grantees must ensure the security of PII and other sensitive information by:

- following TWC Information Security Standards and Guidelines to ensure the security of PII and other sensitive information;
- maintaining PII and other sensitive information in accordance with the TWC standards for information security set forth in WD Letter 13-08, issued April 1, 2008, and entitled "Security of Personal Identity Data," and subsequent updates;
- obtaining PII in conformity with applicable federal and state laws governing confidentiality of information; and
- ensuring that PII and other sensitive information that is transmitted either by e-mail or by mail stored on CDs, DVDs, USB flash drives, or other types of devices is encrypted using a Federal Information Processing Standards (FIPS) 140-2[2]-compliant and National Institute of Standards and Technology (NIST)-validated cryptographic module[3].

NLF: Boards and grantees must ensure that special protections are used with the handling, transportation, storage, retention, and destruction of PII. Each of these will be addressed below.

[2] For more information on FIPS 140-2 standards and cryptographic modules, see FIPS PUB 140-2, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[3] For examples of FIPS 140-2–certified options, see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

NLF: Boards and grantees must ensure that:

- personnel who have access to sensitive, confidential, proprietary, or private data of a confidential nature have implemented the safeguards required to protect the information and are aware of the civil and criminal sanctions in federal and state law for noncompliance with such safeguards;
- policies and procedures exist under which personnel, before being granted access to PII and other sensitive information, acknowledge their understanding of the confidential nature of the information and the safeguards with which they must comply in its handling, as well as liability to civil and criminal sanctions for improper disclosure;
- PII and other sensitive information is accessed only for the purposes set forth in the Agency-Board Agreement or Agency-Grantee Agreement;
- files containing PII are stored in a way that limits access to those with a legitimate need to know;
- PII and other sensitive information is stored in a manner that protects the confidentiality of the records and documents and is designed to prevent unauthorized individuals from retrieving such records by computer, remote access, or any other means;
- if data are downloaded to, or maintained on, mobile or portable devices, the data are encrypted using NIST-validated software products based on FIPS 140-2 encryption;
- PII and other sensitive information is never left in plain sight and unattended;
- PII and other sensitive information obtained through a request is not disclosed to anyone other than an individual or entity authorized by law to receive the information. Individuals authorized by law include, but are not limited to:
  - program staff with a need to know;
  - auditors;
  - state and fiscal monitors; and
  - individuals or entities identified in a signed release from the participant.

NLF: Boards and grantees must be aware that disclosure of PII and other sensitive information also is authorized when required by court order and in response to a subpoena by a governmental entity with subpoena authority. If the disclosure is not accompanied by a court order or a signed written authorization from the individual whose PII is disclosed, Boards and grantees refer subpoenas from attorneys representing civil litigants to the Board's or grantee's attorney to determine objections.

Computers and Data Storage

NLF: Boards and grantees must ensure that:

- only approved computers, servers, media, and software may be used to receive, process, access, and store PII. The Board and grantees must retain control of all work-related PII on all hardware and end-point equipment such as computers, servers, mobile phones, and other storage devices.
- encryption software must be FIPS 140-2 compliant and meet NIST-validated cryptographic standards.
- removable media containing PII are labeled to state the presence of PII.

E-mailing PII

NLF: Boards and grantees must ensure that:

- PII is not sent in the subject or body of an e-mail in clear text;
- PII is sent as an encrypted attachment to an e-mail unless the e-mail software supports encrypting the entire e-mail and its attachments. The password for the attachment must be provided through a separate medium (for example, by a separate e-mail, by phone, or in person);
- When e-mails are sent to multiple customers with identifying information in the body such as "Dear UI Claimant" or "This is related to your TANF Case" the e-mail address of each recipient must be concealed from the other recipients. This is done by putting all recipient addresses in the Bcc field of the e-mail header or by using a software application that sends e-mail to all recipients individually.

Faxing and Printing of PII

NLF: Boards and grantees must ensure that:

- PII and other sensitive information is transmitted only to authorized users; and
- all faxes are sent with a fax cover page that includes the recipient's name and fax number and the sender's name and fax number. The cover sheet must include a confidentiality statement at the bottom of the cover sheet page. (An example of a confidentiality statement is given below.*****);
- when faxing PII to nongovernmental agencies, the sender alerts the recipient before faxing so that the recipient knows not to leave the transmission unattended in an unsecured room;
- in the event of a transmission error, the guidance in the Protection against and Response to Possible Breaches of PII section in this letter is followed;
- printed material and incoming faxes are collected and delivered as quickly as possible;
- the time that PII is left on printers and fax machines is minimized; and
- machines programmed to receive faxes are in a secured or restricted area.

***Confidentiality Notice:** This communication, including any attachments thereto, is intended only for the use of the individual or entity to which it is addressed and contains information that is privileged, confidential, and exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or copying of the message and attachments thereto is strictly prohibited.

Mailing of PII

NLF: Boards and grantees must ensure that:

- PII materials are enclosed in an opaque envelope or container that hides identifying information other than the name and mailing address; and
- the sender uses the US Postal Service's first-class mail, priority mail, or an accountable commercial delivery service.

Transportation of PII

NLF: Boards and grantees must ensure that:

- when PII is transported, the material must remain with the individual and kept from unauthorized disclosure;
- only those employees for whom management has made a designation that it is appropriate for those employees to transport PII are permitted to transport PII;
- all PII removed from an office must be documented using a sign-out and sign-in protocol or other logging method that maintains a record of custody;
- all transportation of PII, including via electronic media, must be documented on a transmittal form and monitored to ensure that PII is properly and punctually received and acknowledged;
- laptops, portable storage devices, mobile phones, and files containing PII must not be left in a vehicle unattended for significant periods of time. If PII must be left in a vehicle for a short time, the PII must be placed in the trunk, if available, or out of plain sight. The vehicle must be locked. Staff transporting files must immediately remove and secure files when they arrive at their destination.

Retention of PII

NLF: Boards and grantees must ensure that:

- PII and other sensitive information is stored in an area that is physically safe from access by unauthorized individuals;
- PII and other sensitive information is kept only for the time required by the Board's retention policy;
- a tracking log of PII stored off-site is maintained;
- if records are stored off-site, the storage facility verifies that it can maintain the security of confidential and sensitive files by meeting the two-barrier minimum standard;
- electronic media and removable media are kept in a secured area under the immediate protection and control of an authorized employee or are locked in a secure place. When not in use, they must be returned promptly to a proper storage area or container;
- when not being used, documents containing PII and other sensitive information are stored under lock and key; and
- PII is stored on hard disks only if office-approved security access control devices (hardware and software) have been installed; are receiving regularly scheduled maintenance, including upgrades; and are actively being used.

Destruction of PII

NLF: Boards and grantees must ensure that:

- when the retention period has ended, PII is destroyed, including degaussing magnetic tape and deleting electronic data, including archived e-mails and other electronic files;
- printed material is destroyed using a shredder or equivalent destruction method. Shredded material must be stored in opaque containers and in a secured or restricted area until removed for permanent destruction;
- recycling bins are not used for disposing of PII;
- computer drives, mobile devices, and other electronic storage devices are wiped

securely of PII before they are reissued to other staff or when they are designated for disposal;
- when using a disposal company, safety measures are in place to maintain the security and confidentiality of files and equipment until they are destroyed.

Protection against and Response to Possible Breaches of PII

NLF: Boards and grantees must ensure that:
- all contracts for services performed by non-Board staff include provisions relating to a breach of PII, including:
  - clearly defined notification requirements;
  - remedies; and
  - penalties; and
- the contract includes a provision for one year of credit monitoring in cases of confirmed PII breaches.

NLF: Boards and grantees must ensure that if staff members suspect or know that PII has been handled in a way that violates policy, or suspect or know of a privacy incident, regardless of the reason or severity, staff must:
- at the time of discovery, secure the PII from further compromise;
- report the incident to the supervisor or (if the supervisor is unavailable or if there is a potential conflict of interest) to the office manager;
- notify TWC immediately of all PII breaches or reasonably assumed release of PII using RSM 3120F. Staff can refer to WD 24-11, Change 1, issued January 17, 2018, and entitled "Reporting Negative Incidents Involving Texas Workforce System Customers—*Update*";
- not compromise the information further by including PII in the incident report;
- document or maintain records relevant to the incident, as they might be required in the privacy incident handling report;
- if the incident was not a breach but PII protection policies were violated, take corrective action to minimize future incidents.

NLF: Boards and grantees must be aware that failure to comply with these requirements, and failure to take appropriate action to prevent any improper use or disclosure of PII and other sensitive information for an unauthorized purpose, is subject to sanctions or other actions as deemed necessary by TWC, up to and including termination of contracts and recoupment of funds, or criminal or civil prosecution. Boards and grantees must hold accountable individuals who improperly use or disclose PII and other sensitive information for unauthorized purposes.

Recommended Best Practices

LF: Boards and grantees are encouraged to employ the following practices to help ensure the security of PII and other sensitive information:
- Before collecting PII or other sensitive information from customers, have the customer sign release forms acknowledging its use, disclosing the entities that will have access to it, and notifying them that in certain circumstances the proper, secure release of their information will be necessary.

- Whenever possible, use unique identifiers such as WorkInTexas.com or The Workforce Information System of Texas (TWIST) identification numbers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier may later be linked to each individual's record. Once the SSN is entered for performance tracking, the unique identifier may be used in place of the SSN for tracking purposes. If SSNs are used for tracking purposes, ensure that they are stored or displayed in a way that disassociates them from individuals, using a truncated SSN or an alternate number such as a TWIST or WorkInTexas.com ID.
- Create procedures to document chain of custody when documents are removed from the premises.
- Whenever possible, ensure that staff computer operations are in an area with restricted access. In those situations, such as work sites where all the requirements of a secure area with restricted access cannot be maintained, the computer equipment and electronic storage media must receive the highest level of protection that is practical.
- Encrypt the entire laptop if this feature is available. If this feature is unavailable encrypt those files containing PII, so that PII will not be compromised if the laptop is lost or stolen.
- Ensure that PII is disposed of using a legitimate and reputable document destruction vendor, preferably one that is National Association for Information Destruction certified.
- When mailing PII, consider double boxed or double wrapping in such a way that if the outer package becomes damaged during transit, then the inner packaging will protect the contents from disclosure.
- Take advantage of tracking options offered by these services to ensure receipt of the mailed materials.
- Turn on the printing of the fax confirmation page to document the successful transmission of the fax. In the event of problems printing confirmation pages, print the fax transmission log to serve as a replacement for individual fax confirmation pages.
- Position the computer monitor so that it is minimally visible to individuals passing by. Use a privacy screen if PII is accessed regularly in an unsecured area where those without a need to know or members of the public can see the monitor screen.
- If PII needs to be stored on a shared network folder, create a limited access subfolder to store that data and provide access privileges only to those who have a need to access the information.
- Lock the computer when away from the duty station.

INQUIRIES:

Send inquiries regarding this WD Letter to wfpolicy.clarifications@twc.state.tx.us.

REFERENCES:

Privacy Act of 1974, as amended, 5 USC §552a

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf

US Department of Labor Employment and Training Administration Training and Employment Guidance Letter 39-11, issued June 28, 2012, and entitled "Guidance on the Handling and Protection of Personally Identifiable Information (PII)," http://wdr.doleta.gov/directives/attach/TEGL/TEGL_39_11_Acc.pdf

Federal Information Processing Standards Publication 140-2

Texas Government Code §552.137

WD Letter 13-08, issued April 4, 2008, and entitled "Security of Personal Identity Data"

Texas Workforce Commission Information Security Standards and Guidelines, https://intra.twc.state.tx.us/intranet/its/docs/iris_standard.pdf