PERSONALLY IDENTIFIABLE INFORMATION AND CONFIDENTIAL INFORMATION

Federal law requires personally identifiable information (PII) and other sensitive information be protected.

There are two types of PII – protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.

1. Protected PII – information that, if disclosed, could result in harm to the individual whose name or identity is linked to the information. Examples of protected PII include, but are not limited to, social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, biometric identifiers (fingerprints, iris scans, etc.), medical history, financial information and computer passwords.
2. Non-sensitive PII – information that, if disclosed, by itself could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples include first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

REQUIREMENTS

Federal Requirements include:

- The ETA has established the following requirements for the handling of PII.
- All PII and other sensitive data transmitted via email or stored CDs, DVDs, thumb drives, etc. must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. Unencrypted sensitive PII cannot be emailed.
- Data must be processed in a manner to protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records.
- DLR employees must ensure privacy of all PII obtained from participants and/or other individuals and protect such information from unauthorized disclosure.
- PII data must be stored in an area physically safe from access by unauthorized persons at all times. Accessing, processing and storing of ETA grant PII data on personally owned equipment at off-site locations is prohibited.
- DLR employees and other personnel who will have access to PII must be advised of the confidential nature of the information, the safeguards to protect the information and the civil and criminal sanctions for noncompliance with such safeguards. Personnel must acknowledge their understanding of these compliance requirements and their liability for improper disclosure.
- Data may not be obtained or used for any purpose other than those required by the programs. Access to data is restricted to only those individuals who need it in their official capacity to perform duties in connection with the scope of work.

DLR release of information requirements Include:

- Job service offices are authorized to share information with other state and federal agencies with the exception of the new-hire information. This information may only be released by the manager of the New-Hire Program.
- Prior to releasing a job seeker's information, an authorization form must be signed by the job seeker.
- Requests for information from local law-enforcement agencies should be accommodated without compromising registrant confidentiality. Requests for registrant files, documents or other printed personal information shall not be released without a subpoena.

- The Director of Employment Services should be informed of requests for information made by law enforcement, as well as requests for information made by subpoena. If in doubt about a situation, the Director of Employment Services should be contacted.
- The various SDWORKS screens available contain confidential information that can only be used by assigned staff and only for authorized purposes. The available screens are not to be printed, duplicated or disseminated in any unauthorized manner. This includes job orders, job seeker/participant data, business data and Reemployment Assistance (RA) benefits.

Department of Social Services (DSS) and the Department of Corrections (DOC) have read-only access to the SDWORKS system. Responsibility accompanies this privilege. Any abuse of this privilege will result in termination of access to the SDWORKS system. Other legal implications may result with inappropriate usage.

Use appropriate methods for destroying sensitive PII on paper, such as shredding, and securely deleting sensitive electronic PII.

SOCIAL SECURITY NUMBERS

SOCIAL SECURITY NUMBERS

All DLR staff have a responsibility to keep Social Security Numbers (SSNs) of job seekers and other individuals secure.

DLR prohibits the disclosure of SSNs to unauthorized persons or entities. DLR employees will not knowingly display, disclose, transfer, or unlawfully use the SSN of any employee, student, or other individual in any manner that violates the Social Security Protection Act of 2004 or the Privacy Act of 1974.

SSNs should only be collected where required by federal or state law. If a unique personal identifier is needed, a substitute for the Social Security number shall be used in its place.

Documents, materials, or computer screens displaying SSNs shall be kept out of public view at all times.

Documents containing SSNs shall only be sent where permitted by state and federal law. A SSN may be included in a mailed document where:

- It is sent as part of an application or enrollment process initiated by the individual.
- It is sent to establish, confirm the status of, service, amend or terminate an account, contract, employee or health insurance benefit – or to confirm the accuracy of a Social Security number of an individual who has an account, contract, policy, or employee or health insurance benefit.
- It is sent for the purpose of compliance with proper administration of the RA program.
- It is contained in a public record and is mailed in compliance with the Freedom of Information Act. Otherwise, the Social Security number shall be redacted.
- It is mailed by, or at the request of, an individual whose Social Security number appears in the document or information of his or her parent or legal guardian.
- The number shall not be revealed through the envelope window or be visible from the outside of the envelope.

Full SSNs shall not be sent through email. Simply state the individual's first and last name and last four digits of his/her Social Security number. However, when sent for business purposes only, full SSNs may be sent through internal email between the RA Division and job service office staff only.

When it is necessary to provide a full SSN or other PII to an outside entity, e.g. an insurance company overseeing a workers' comp claim, the PII may be sent if Voltage Encryption email is utilized by DLR personnel. Do not send any emails to email domains outside of the state's domain without using encryption software, such as Voltage.

DLR employees shall not disclose any SSN over the telephone or leave a voice mail message disclosing any SSN. If a SSN must be faxed, the fax message shall be accompanied by a transmittal sheet which includes a "Confidential Notice" stating the information included is intended to be privileged and confidential and it is only intended for the use of the individual or entity named on the transmittal sheet.

All documents or files containing SSNs shall be stored in a physically secure manner. SSNs shall not be stored on computers or other electronic devices not secured against unauthorized access. When erasing Social Security numbers from a laptop or desktop computer, staff shall ensure the number was erased completely, including from the recycle bin.

Documents containing Social Security numbers shall not be thrown away in the trash, but instead discarded or destroyed only in a manner that protects their confidentiality, such as shredding.

Pseudo Numbers for Job Seekers

Although the SSN is helpful, it is not required to register a job seeker into SDWORKS. If the seeker does not wish to share it, a pseudo-SSN will be generated by SDWORKS. If the client will be enrolling in certain programs, the SSN will be required.

TEGL 39-11