North Central Counties Consortium
Personally Identifiable Information (PII) Procedure

Purpose

The purpose of this policy is to establish local practices that protect sensitive information provided by applicants, participants, employers, and employees from improper use, disclosure, or transmission.

Background/Definitions

The Privacy Act of 1974 safeguards individuals against invasions of privacy when sensitive information is required for official use. North Central Counties Consortium (NCCC) may have large quantities of sensitive information relating to the organization, staff, subrecipients, partner organizations, and individual program participants by virtue of its status as a steward of federal funding. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, contract files, and other sources.

Sensitive Information - any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.

Personally Identifiable Information (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.

Protected PII - information that if disclosed could result in harm to the individual whose name or identity is linked to that 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, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information, and computer passwords.

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 of non-sensitive PII include information such as 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 PII.

The Workforce Innovation and Opportunity Act (WIOA) requires that all sensitive information:

- Is collected, used, and stored in a manner that ensures it will not be accessible to anyone not authorized to access it;
- Is not collected unless needed for the provision of some service or to determine eligibility for a program;
- Is not used for any purpose other than the program or service for which it was collected, unless the subject of the information (if the subject is an adult), or a parent of the subject (if the subject is a minor or dependent), provides consent for the information to be shared;
- Can be released to the subject of the information upon his or her request;
- Is not accessible to anyone other than those authorized to access it (including agents of oversight and regulatory entities, and in cases in which the information has been subpoenaed, parties to the legal matter); and
- Is published only in aggregate form, preventing readers from being able to identify, or reasonably infer the identity of, any individual subject.

Local Policy

NCCC's policy is to make every reasonable effort to safeguard sensitive information, including PII. All staff and subrecipients shall strictly adhere to state and federal regulations pertaining to privacy, confidentiality, and record security. In addition to the minimum requirements outlined above, NCCC shall:

- Utilize appropriate computer, network, and internet security controls;
- Dispose of PII in a safe and secure manner;
- Follow the Social Security Administration's (SSA's) safeguarding policy for beneficiary's PII;
- Ensure that NCCC and subrecipient personnel acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply in their handling of such data as well as the fact that they may be liable for civil and criminal sanctions for improper disclosure (TEGL39-11);
- Allow EDD to conduct onsite inspection during regular hours for the purpose of conducting audits and/or conducting other investigations to assure that NCCC and subrecipients are complying with confidentiality requirements. NCCC and its subrecipients must make applicable records available to authorized persons for the purpose of inspection, review, and/or audit (TEGL39-11); and
- Will retain data from EDD only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal records retention requirements, if any. NCCC and subrecipients will destroy all data, including the degaussing of magnetic tape files and deletion of electronic data (TEGL39-11).

In accordance with the Code of Federal Regulations, 29 CFR 38.41, any medical or disability-related information obtained about a particular individual, including information that could lead to the disclosure of a disability, must be collected on separate forms. All such information,

whether in hard copy, electronic, or both, must be maintained in one or more separate files, apart from any other information about the individual, and treated as confidential. Whether these files are electronic or hard copy, they must be locked or otherwise secured (for example, through password protection).

Separate file contents:

- Any identifying information must be redacted;
- Medical or disability-related information collected on the WIOA application;
- **Hard copy case notes pertaining to a medical or disability-related condition. Case notes pertaining to a medical or disability-related condition entered into the CalJOBS system must be suppressed;**
- ISS with disability information; and
- EV09 Applicant/Case Manager Statement of Barriers Form with pregnancy or disability information only.

DD Form 214 identifying an individual's disability must be redacted and kept in the main file.

Documents containing sensitive information, including full social security numbers, must be encrypted prior to sending electronically with either document encryption/password protection or by secure, encrypted electronic mail (e-mail). E-mail containing sensitive information, including full social security numbers, must be encrypted. It is permissible to e-mail a participant's name and only the last four digits of their social security number without encrypting the e-mail.

Knowledge of disability status or medical condition and access to information in related files. Persons in the following categories may be informed about an individual's disability or medical condition and have access to the information in related files under the following listed circumstances:

(A) Program staff who are responsible for documenting eligibility, where disability is an eligibility criterion for a program or activity.

(B) First aid and safety personnel who need access to underlying documentation related to a participant's medical condition in an emergency.

(C) Government officials engaged in enforcing this part, any other laws administered by the Department, or any other Federal laws. See also § 38.44.

<u>Ticket to Work Program</u>

As an approved Employment Network (EN), NCCC shall protect Ticket Program beneficiary's PII in accordance with Part III, Section 6 and Part IV, Section 3 of the EN agreement. NCCC and its subrecipients shall:

- Use and access beneficiary information only for the purposes of SSA's Ticket Program;
- Dispose of beneficiary information in a safe and secure manner;
- Not duplicate or disseminate beneficiary information outside the EN's organization;
- Provide physical safeguards for protecting the security of beneficiary information, including restricting access only to authorized employees and officials who have received their security clearance and who need the information to perform their official duties in connection with SSA's Ticket Program;
- Store beneficiary information in a physically secure area and assure that it cannot be accessed and retrieved by unauthorized personnel; and
- Ensure that all personnel who have access to beneficiary information have met the security suitability requirements and have complied with SSA's security awareness and Federal Information Security and Management Act (FISMA) training requirements.

According to the SSA NCCC's organizational e-mail system is deemed not to be secure. Staff and subrecipients may send e-mail messages transmitting PII **only if the PII is entirely contained within an encrypted attachment. None of the PII may be in the body of the e-mail or within an unencrypted attachment.**

Staff with limited access to Ticket Program beneficiary's PII solely through a beneficiary's self-disclosure of such information as part of the service delivery process would not need to complete the Social Security suitability process. Such staff would, however, need to follow the safeguarding strategies outlined above.

Instructions for Reporting Lost, Compromised, or Potentially Compromised PII

When an employee or subrecipient becomes aware or suspects that PII has been lost, compromised, or potentially compromised he/she shall provide **immediate** notification of the incident to NCCC's Equal Opportunity Officer (EOO). The employee or subrecipient shall provide complete and accurate information including:

- A description of the loss, compromise, or potential compromise
- A description of the safeguards used (locked cabinet, redacted PII, password protection, etc.)
- Whether the employee or subrecipient has contacted or been contacted by any external organization (law enforcement, media, etc.)
- Whether or not the PII of Ticket Program beneficiaries was affected

In the event the loss, compromise, or potential compromise includes the PII of Ticket Program beneficiaries, additional reporting requirements apply (see Section 3.K of the EN agreement). Finally, the employee or subrecipient shall limit disclosure of the details about an incident to only those with a need to know.

References

The Privacy Act of 1974 (Public Law 93-579)
WIOA (Public Law 113-128) Section 185
TEGL No. 5-08
TEGL No. 39-11
OMB Memorandum M-07-16
Uniform Guidance 2CFR Part 200.79 & 200.82
EN RFQ-12-0010L 8-27-12
Code of Federal Regulations 29 CFR 38.41-38.45